VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Bezpečnost na mobilních zařízeních s operačním systémem Android

Security on Mobile Devices Running OS Android

Student: Bc. Ondřej Gajda

Vedoucí diplomové práce: doc. Ing. Milena Tvrdíková, Csc.

Ostrava 2014

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání diplomové práce

Student: **Bc. Ondřej Gajda**

Studijní program: N6209 Systémové inženýrství a informatika

Studijní obor: 1802T001 Aplikovaná informatika

Téma: Bezpečnost na mobilních zařízeních s operačním systémem Android
Security on Mobile Devices Running OS Android

Zásady pro vypracování:

1. Úvod
2. Teoretická východiska OS pro mobilní zařízení
3. Analýza bezpečnosti OS Android
4. Návrh preventivních opatření a doporučení pro práci s OS Android
5. Vyhodnocení efektu z realizace opatření
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

HOOG, Andrew. *Android Forensics: Investigation, Analysis, and Mobile Security for Google Android*. Amsterdam: Elsevier, 2011. ISBN 978-1-59749-651-3.
SIX, Jeff. *Application security for the Android platform: Investigation, Analysis, and Mobile Security for Google Android*. Sebastopol: O'Reilly, 2011. ISBN 978-1-449-31507-8.
DUBEY, Abhishek and Anmol MISRA. *Android Security: Attacks and Defenses*. Boca Raton: CRC Press, 2011. ISBN 978-143-9896-464.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **doc. Ing. Milena Tvrdíková, CSc.**

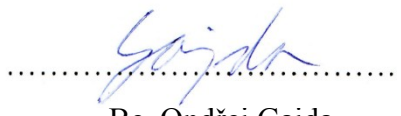
Datum zadání: 22.11.2013
Datum odevzdání: 25.04.2014

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA * OSTRAVA 1 Ekonomická fakulta

Ing. Petr Rozehnal, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

Prohlašuji, že jsem celou práci, včetně všech příloh, vypracoval samostatně.



Bc. Ondřej Gajda

V Ostravě dne 25. 4. 2014

Poděkování

Tímto bych rád poděkoval vedoucí mé diplomové práce doc. Ing. Mileně Tvrdíkové, CSc. za odbornou pomoc, poskytnuté rady a inspiraci.

Obsah

1 Úvod

Tempo vývoje nových technologií stále roste a to, co se zdálo být ještě před pár lety nemožným, se stalo realitou. Je fascinující jakou evolucí prošly mobilní zařízení, než se staly běžnou součástí našich životů, našimi pomocníky v osobním i profesním životě. Pro většinu lidí se jedná o neodlučitelné společníky a jen zřídka se od nich nacházejí dále než jen pár metrů a to i během spánku.

Moderní mobilní zařízení jsou jedna z nejosobnějších věcí, které kdy člověk vlastnil. Tyto přístroje nevelkých rozměrů obsahují jména, telefonní čísla a adresy rodinných příslušníků, přátel ale i kolegů z práce či zákazníků, stovky fotografií, historii prohlížení webového obsahu ale i historii polohy zařízení, prozrazující, kde se v danou dobu zařízení nacházelo. Tím však výčet osobních informací, které mohou být zcizeny, zdaleka nekončí. Je stále běžnější používat mobilní zařízení pro uskutečňování plateb, ať již prostřednictvím internetového bankovnictví nebo pomocí elektronických peněženek. Je tedy zřejmé, že uživatel, aniž by si to třeba uvědomoval, se má o co obávat a měl by vynaložit alespoň minimální úsilí o zabezpečení dat svého mobilního zařízení. Jejich zcizení může proběhnout pouze dvěma způsoby. Tím prvním je krádež fyzického zařízení a jeho případné zneužití. Druhou možností je napadení systému prostřednictvím internetového připojení a podvodných aplikací.

Počet mobilních zařízení s operačním systémem Android stále roste a bylo by naivní domnívat se, že majiteli těchto zařízení jsou pouze lidé srozuměni s riziky a podnikají tak veškeré aktivity v souladu se základními bezpečnostními pravidly. S rostoucí popularitou a množstvím mobilních zařízení rovněž roste množství příležitostí pro případné útočníky, kteří se tak zaměřují na nejrozšířenější platformu.

Cílem této diplomové práce je analyzovat bezpečnost mobilního operačního systému Android, upozornit na škodlivý software, který může ohrozit data uložená v mobilních zařízeních, vypracovat návrh řešení bezpečnostních opatření a vyhodnocení efektu z realizace těchto opatření na základě vlastního testování. Součástí práce je rovněž dotazníkové šetření určené pro získání přehledu o povědomí uživatelů o bezpečnostních hrozbách vyplývajících z užívání mobilních zařízení.

2 Teoretická východiska OS pro mobilní zařízení

Mobilní operační systém je definován jako základní programové vybavení daného mobilního zařízení, které je zavedeno do jeho paměti při startu a zůstává v činnosti až do jeho vypnutí. Zde podobnost s desktopovými operačními systémy nekončí. Stejně jako desktopové OS i mobilní operační systémy umí pracovat s internetovým připojením, s multimediálními a kancelářskými nástroji apod., přičemž navíc poskytují uživateli služby využívající hardwarové vybavení přístroje, jako jsou dotykové obrazovky, GPS přijímač sloužící pro určení polohy a navigaci, Bluetooth a Wi-Fi direct pro přenos souborů a další.

2.1 Vývoj mobilních operačních systémů

Mezi historicky nejstarší mobilní operační systémy se řadí vestavěné systémy, které byly využívány v prvních mobilních telefonech a s operačními systémy, tak jak je známe dnes, neměly mnoho společného. Takovýto systém udržoval zařízení v chodu a poskytoval základní funkce jako je volání na jiná zařízení, zasílání SMS a ukládání kontaktů. V listopadu roku 1992 bylo společností IBM představeno zařízení, které lze označit jako první smartphone. Přístroj vážící rovných 510g nesl název IBM Simon a disponoval dotykovým panelem, operační pamětí 1 MB a pamětí pro data téže velikosti. Operačním systémem byl Datalight ROM-DOS, který umožňoval uživateli přijímat a zasílat faxy a e-maily. Mezi další aplikace patřil kalendář, kalkulátor, adresář kontaktů, světový čas a za zmínku rovněž stojí funkce rozpoznávání ručně psaného písma.

Společnost Palm, Inc. uvedla v roce 1996 na mezinárodní trh systém Palm OS, který byl určen pro tzv. PDA, česky označován také jako osobní digitální pomocník. Toto zařízení kapesních rozměrů do jisté míry bylo schopné zastoupit klasický stolní počítač. Zde je důležité uvést, že společnost Palm, Inc. nebyla první, která uvedla na trh PDA. O tři roky dříve, v roce 1993, vyvinula firma Apple Computer, nyní již Apple Inc., přístroj nazvaný Apple Newton, který využíval ke své práci operační systém Newton OS. Tento systém byl napsán v programovacím jazyce C++ a byl naprogramován pro efektivní využití operační paměti a nízkou spotřebu energie. Podobně jako operační systém Datalight ROM-DOS

disponoval funkcí rozpoznávání ručně psaného písma, dále umožňoval třídění složek a souborů a následně tyto soubory tisknout pomocí externí tiskárny, otáčení obrazovky pro pohodlnější psaní textu a kreslení pomocí stylusu a předinstalovaný program pro čtení elektronických knih rozšiřoval možnosti využití. Vzhledem ke své vysoké ceně a rozměrům však nedosáhl Apple Newton takové obliby jako právě PDA s operačním systémem Palm OS. Palm OS nabízel obdobné funkce jako Newton OS, avšak jeho tvůrci už pamatovali na bezpečnost a zakomponovali do systému nástroj pro skrytí záznamů v přístroji. Následné verze systému přinesly podporu barevných displayů, použití externích paměťových karet, sdílení souborů pomocí infračerveného záření a Bluetooth, přístupu k síti Internet a další.

Důležitou roli ve vývoji mobilních operačních systémů sehrál systém Microsoft Windows CE vyvinutý společností Microsoft, který byl představen ve stejném roce jako operační systém Palm OS a byl rovněž určen pro mobilní zařízení PDA. Systém se velmi podobal operačnímu systému Microsoft Windows 95 určenému pro stolní počítače, obsahoval známou nabídku Start, nástroj pro prohledávání složek souborů, nabídku ovládací panely a další. Pro kancelářskou práci byly určeny programy Microsoft Word a Microsoft Excel, rovněž známé z desktopového operačního systému. Další verze přinesly podporu protokolu TCP/IP a internetový prohlížeč Internet Explorer, podporu USB a rozšíření kompatibility s různými typy hardwaru. Mobilní operační systém Microsoft Windows CE rovněž posloužil jako základ pro další mobilní operační systémy vyvíjené společností Microsoft. Prvním uvedeným byl v polovině roku 2000 systém Pocket PC 2000. S přepracovaným ovládáním a grafickým rozhraním se měl stát přímou konkurencí pro operační systém Palm OS. Další verze přinesly podporu více formátů multimédií, podporu konektivity prostřednictvím Wi-Fi a Bluetooth, vylepšenou synchronizaci zařízení se stolním počítačem atp. Systém Pocket PC 2000 se dočkal svého nástupce v roce 2001, který byl představen pod názvem Pocket PC 2002. Jedná se o poslední systém vyvinutý společností Microsoft nesoucí ve svém názvu Pocket PC a zároveň o první mobilní operační systém společnosti Microsoft, který byl určen i pro mobilní telefony. Roku 2003 byl uveden na trh mobilní operační systém Windows Mobile 2003. Tento systém přinesl, kromě velmi výrazných změn grafického rozhraní, podporu práce s 3D grafikou, sdílení vzdálené plochy pomocí protokolu RDP a byl jedním z prvních systémů na mobilních telefonech označovaných jako smartphone, jehož stručná definice se nachází v následné kapitole. Windows Mobile využívá k zajištění bezpečnosti dat systém oprávnění, ověřování certifikátů a podpisů aplikací. Datová komunikace prostřednictvím sítí je šifrována pomocí SSL protokolu. Systém Windows Mobile 2003

se dočkal celkem pěti dalších nástupců, jejichž vývoj byl ukončen v roce 2010. Za nepřímého pokračovatele se považuje systém Windows Phone, který byl uveden v tomtéž roce, tj. 2010. Windows Phone vychází z šesté verze systému Microsoft Windows CE uvedené roku 2006, která obsahovala kompletně přeprogramované jádro systému, což mělo za důsledek výrazné zvýšení počtu souběžně běžících procesů, větší podporu multimédií a podporu technologií jako např. šifrování WPA2 atd. Windows Phone se liší výraznou grafickou úpravou, podporou dotykového ovládání pomocí prstu a přizpůsobením na výkonnější hardware. Tento systém je podrobněji rozepsán v následujících kapitolách.

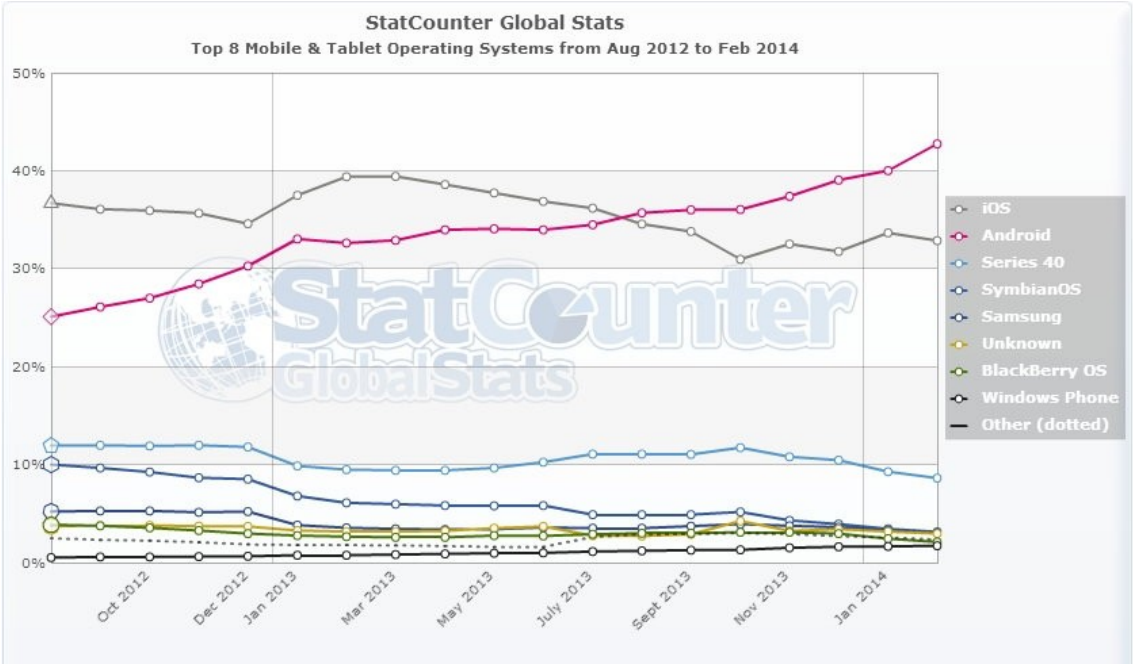
Velké popularity a masového rozšíření dosáhl rovněž mobilní operační systém Symbian vyvíjený od roku 1998 organizací Symbian Ltd. a následně neziskovou organizací Symbian Foundation, jejíž členy byly společnosti Nokia, Sony Ericsson, Motorola, Samsung Electronics a další. Tento systém vycházel z operačního systému určeného pro mobilní zařízení, Epoc, vyvíjeného na konci 80. a počátku 90. let 20. století společností Psion a první verzi systému Symbian, psaného v programovacím jazyce C++, lze označit jako šestou verzi systému Epoc. Nokia v roce 2001 uvedla na trh první zařízení s tímto operačním systémem a ještě v tomtéž roce představila i své uživatelské prostředí Series 60 pro Symbian. Další uživatelská prostředí byla např. UIQ, používané převážně společností Sony Ericsson, nebo MOAP, určené pro japonský trh. Důvěra společnosti Nokia vkládaná v systém se projevila výrobou přes sto různých mobilních zařízení právě s tímto systémem a v roce 2008 odkoupením zbývajících akcií od ostatních společností. Systém Symbian disponoval uživatelsky přívětivým prostředím a byl v různých verzích přizpůsoben jak pro dotykové ovládání, tak pro ovládání pomocí hardwarové klávesnice. Právě tyto vlastnosti v kombinaci s podporou 48 světových jazyků mají za následek světové rozšíření systému. Symbian dále svým uživatelům nabízel podporu wi-fi připojení, přehrávání multimediálních souborů, podporu multitaskingu (běh více aplikací najednou), instalaci dalších aplikací a her. Nejdůležitějšími prvky bezpečnostního modelu systému Symbian jsou tříúrovňový model důvěry, systém oprávnění a ověřování podpisů aplikací a přístupový systém k důležitým souborům. Avšak otevřenost a veřejně dostupný zdrojový kód systému umožňuje útočníkům snáze vytvořit škodlivý software. V roce 2004 se objevil první virus pro chytré telefony a to právě v zařízeních s operačním systémem Symbian. Virus pojmenovaný Cabir se šířil pomocí technologie Bluetooth metodou bluejacking. Metoda spočívala v prohledávání svého okolí a hledání mobilních telefonů se zapnutým Bluetooth s nastavenou viditelností pro ostatní zařízení a výše zmíněnou nadstavbou pro OS Symbian Series 60. Virus se maskoval jako

utilita Caribe Security Manager, která tvořila součást bezpečnostního software Symbianu. Přestože jediná úloha byla neustále využívat Bluetooth, odborná veřejnost varovala před možným rozšířením virů, malwaru a jiných škodlivých programů na mobilní platformu. V roce 2011 oznámila společnost Nokia nově vzniklé partnerství se společností Microsoft, které vedlo k nasazení mobilního operačního systému Windows Phone jako primárního systému pro jejich další zařízení a na začátku roku 2014 byla ukončena podpora Symbianu. Jako pravděpodobný důvod k tomuto kroku je označován konkurenční tlak vyvolaný nárůstem popularity konkurenčních systémů Android a iOS.

Poněkud odlišným vývojem prošel mobilní operační systém BlackBerry OS. V roce 1999 byl kanadskou společností Research In Motion představen digitální pager se systémem BlackBerry OS 1.0, který umožňoval obousměrnou komunikaci pomocí textových zpráv. Telefonní funkce přibyla až v roce 2002, v systémové verzi 3.6. Nová verze navíc umožňovala zasílání emailů, faxů, připojení na internet atp. Zařízení se systémem BlackBerry si získala oblibu převážně u obchodníků a manažerů, a to zejména kvůli způsobu, jakým tyto zařízení pracují. Většinu funkcionalit totiž zprostředkovává server, a to buď server společnosti Research In Motion nebo dané firmy, v níž je zařízení využíváno. Prakticky veškerá síťová komunikace prochází šifrovaně právě tímto serverem, který za uživatele kontroluje mailové schránky, tzv. mailboxy, předzpracovává webové stránky, což má za následek rychlejší zobrazení obsahu, synchronizuje kalendář, atp. Ve své podstatě se jedná o cloudové řešení SaaS, Software as a Service, česky Software jako služba. Veškerá data odesílána na server jsou šifrovaná pomocí Triple DES nebo AES algoritmů symetrického šifrování. Toto zabezpečení dat tvoří společně s ověřováním podpisů aplikací základ bezpečnostního modelu systému BlackBerry OS, který bývá označován jako jedna z nejbezpečnějších mobilních platforem. Dnes je systém vyvíjen společností BlackBerry Ltd.

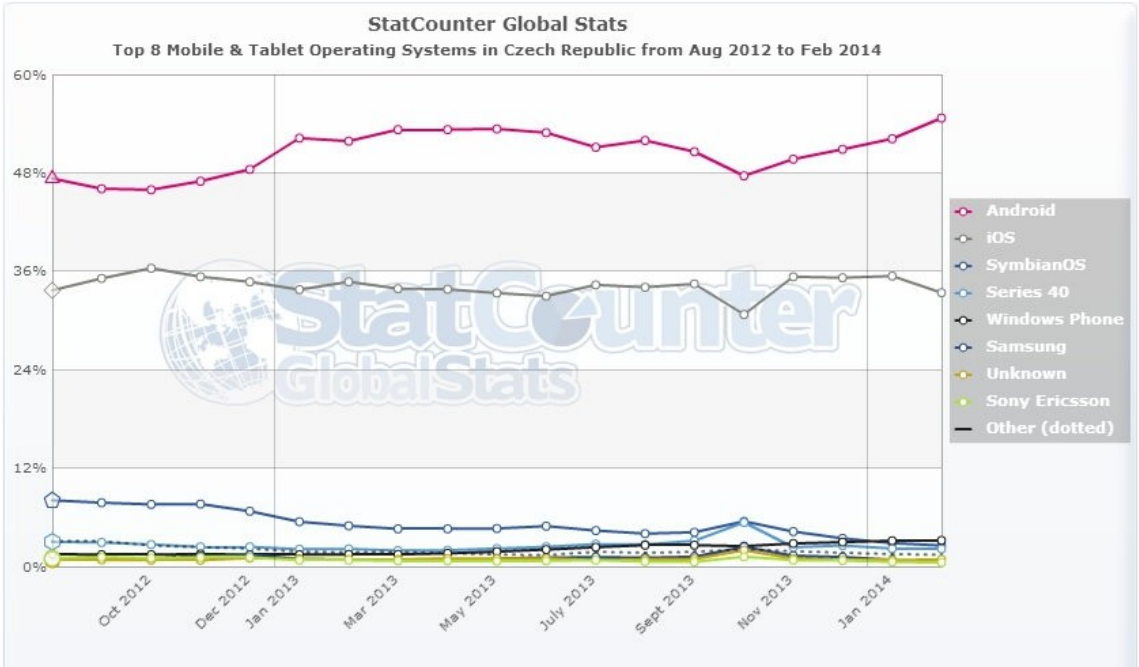
V dalších letech se vývoj mobilních operačních systémů značně urychlil, změnil se trh s mobilními zařízeními, vzrostla jejich popularita a vznikly i operační systémy zcela nové jako např. China Operating System s posvěcením čínské vlády, Tizen, Firefox OS a další. Velkou roli na poli mobilních operačních systémů sehrála společnost Apple Inc. se svým systémem iOS a společnost Google se systémem Android. Oběma je věnován patřičný prostor v následujících kapitolách.

Na grafech níže je vyobrazen vývoj růstu nejpoužívanějších mobilních OS ve světě a České republice.



Graf 2.1.1 - Vývoj růstu jednotlivých mobilních OS celosvětově

[zdroj: http://gs.statcounter.com/#mobile+tablet-os-ww-monthly-201208-201402]



Graf 2.1.2 - Vývoj růstu jednotlivých mobilních OS v ČR

[zdroj: http://gs.statcounter.com/#mobile+tablet-os-CZ-monthly-201208-201402]

Jak je z grafu výše patrné, v České republice dominuje na mobilních zařízeních operační systém Android. Pomyslnou druhou příčku obsadil systém iOS společnosti Apple Inc. a na počátku roku 2014 lze pozorovat nárůst podílu Windows Phone, který se tímto stal třetím nejpoužívanějším mobilním operačním systémem v České republice.

2.2 Android

Obr. 2.2.1 - Logo Android

[zdroj:http://developer.android.com/images/brand/Android_Robot_200.png]

OS Android lze stručně popsat jako otevřený, neboli open-source, mobilní operační systém, který je založen na jádře operačního systému Linux, programovaný v jazyce Java.

S operačním systémem Android se lze setkat v mobilních telefonech, tabletech, netboocích, chytrých hodinkách, fotoaparátech, čtečkách elektronických knih, set-top boxech, herních konzolích a dokonce v palubních počítačích automobilů. Takto širokého využití OS Android je dosaženo hlavně díky otevřenosti tohoto systému a dostupnosti zdrojového kódu, který dává vývojářům možnost provádět prakticky jakékoliv potřebné úpravy. Právě tato otevřenost je z hlediska bezpečnosti předmětem mnoha kritik.

Historie OS Android se začíná psát roku 2003 ve státu Kalifornie, USA, kdy byla založena společnost Android, Inc. Zakladateli byli Andy Rubin, Rich Miner, Nick Sears a Chris White. V srpnu roku 2005 byla tato začínající společnost odkoupena firmou Google Inc. a Andy Rubin byl dosazen do vedení vývojového týmu. Ten poté vyvinul platformu založenou na Linuxovém jádře a společnost Google obstarala několik patentů z oblasti mobilních technologií. Andy Rubin oznámil 5. listopadu 2007 spojení sil s nově vzniklým společenstvím Open Handset Alliance, které si kladlo za cíl urychlení inovací v oblasti mobilních technologií a nabídnutí spotřebitelům levnější a lepší mobilní platformy se vším, co k ní patří. Při zakládání mělo konsorcium 34 členů, kromě Google např. Samsung, Intel, Texas Instruments a další. Na konci roku 2013 čítalo společenství Open Handset Alliance 84 členů, společností, z oblasti vývoje mobilních a počítačových technologií. Prvním zařízením se systémem Android se stal mobilní telefon T-Mobile G1, označovaný rovněž jako HTC Dream, který byl uveden v říjnu roku 2008 ve Spojených státech amerických[1]. Aby podpořil vývoj aplikací pro svůj systém, a tím se stal zajímavějším pro uživatele, vyčlenil Google jeden milion dolarů na odměny autorům nejinovativnějších aplikací a uvolnil tzv. SDK, software development kit, základní nástroje pro vývojáře. SDK např. obsahuje nástroj na odladění programu, debugger, základní knihovny, ukázky kódu atd. V srpnu stejného roku oznámila společnost Google dostupnost oficiální distribuční služby pro operační systém Android, Android Market, kde vývojáři mohli začít nahrávat své aplikace a nabízet je tak uživatelům ke stažení. První verze služby Android Market nepodporovala placené aplikace, a proto byl veškerý obsah uvolňován zdarma. V současné době se tato

služba jmenuje Google Play a obsahuje více než milion různých aplikací, které jsou šířeny zdarma, placeny nebo jsou zdarma ke stažení, ale obsahují platby uvnitř aplikace, tzv. in-app purchases. Kromě aplikací jsou zde dostupné i elektronické verze knih, hudba, tapety atp.

S každou následující verzí mohli uživatelé pozorovat změny vzhledu i rozšíření nabídky funkcí. Nejnovější verze nese označení 4.4 Kit Kat a jedná se již, jak první číslo z dvojčíslí napovídá, o čtvrtou verzi systému. Slovní část označení je inspirováno čokoládovými tyčinkami stejného názvu, jelikož vývojáři pojmenovávají všechny verze podle cukrovinek.

Obliba mobilního operačního systému společnosti Google mezi vývojáři a koncovými uživateli vzrostla natolik, že v druhé polovině roku 2013 bylo dosaženo jedné miliardy aktivovaných zařízení s tímto systémem. Statisticky Android vede na celosvětovém i českém trhu v kategorii nejpoužívanějšího mobilního systému. Vzhledem k faktu, že tato diplomová práce pojednává o bezpečnosti na mobilních zařízeních s operačním systémem Android, je architektuře systému a modelu zabezpečení věnovaná třetí kapitola.

2.3 iOS

Obr. 2.3.1 - Logo iOS

[zdroj:http://images.apple.com/support/ipad/assistant/images/ios_icon_20110921.png]

Mobilní operační systém iOS je uzavřený systém vyznačující se zejména svou stabilitou a unifikovaným rozhraním.

Na počátku roku 2007 byl světu představen mobilní telefon iPhone společnosti Apple Inc. V telefonu se nacházel do té doby jinde neviděný mobilní operační systém odvozený od operačního systému Mac OS X, iPhone OS (později iOS), vyvinutý rovněž touto společností. Oba systémy jsou založeny na jádru Unixu a používaly i stejné nástroje. Na rozdíl od společnosti Google, neměli zástupci Applu původně v plánu uvolnit SDK, a nebylo tedy umožněno doinstalovat aplikace třetích stran. To se však změnilo na počátku roku 2008. I přes značná omezení, která se u konkurence nenacházela, jako byla nemožnost umístění ikon na domovské obrazovce dle libosti uživatele, kopírování a následné vkládání textu, připojení příloh k emailům nebo třeba chybějící multitasking, zaznamenal iOS velmi výrazný úspěch. Velkou zásluhu nese již zmíněný mobilní telefon iPhone, jehož veškeré hardwarové vybavení bylo podřízeno systému iOS a tím byl zajištěn spolehlivý a rychlý chod zařízení jako celku. Odborná veřejnost hovořila o revoluci na trhu mobilních telefonů.

Společnost Apple Inc. v roce 2008 poskytla, kromě SDK pro vývojáře, oficiální distribuční službu nazvanou App Store, která umožňuje instalovat i aplikace třetích stran přímo v zařízení bez nutnosti připojení ke stolnímu počítači. Kromě aplikací zde může uživatel stahovat i další digitální obsah, jako např. elektronické verze knih a časopisů, videa nebo hudbu. Zástupci společnosti Apple věnují patřičnou pozornost bezpečnosti obsahu služby App Store a podrobují jej přísnému a pečlivému testování pomocí softwarových nástrojů a odhalují tak škodlivý kód. V následujících letech byly uvolněny další verze systému iOS, v nichž přibyly funkce a služby, jako např.: zasílání MMS zpráv, zobrazování notifikací (textové upozornění aplikace), ovládání hlasem, video chat atp. Mobilní telefon iPhone nezůstal jediným zařízením, kde se lze se systémem iOS setkat. Systém byl uveden i na tablet nesoucí název iPad, v přenosných multimediálních přehrávačích iPod touch a v tzv. Apple TV, multimediálním centru, které umožňuje přehrávat filmy, videa a sdílet obrazovku ostatních zařízení společnosti Apple Inc. Všechna uvedená zařízení jsou vyvinuta společností Apple Inc. a v souladu s jejich filozofií jsou jediná, kde se lze s iOS setkat. Poslední verze nese číselné označení 7 a byla uvedena v roce 2013.

2.3.1 Zabezpečení

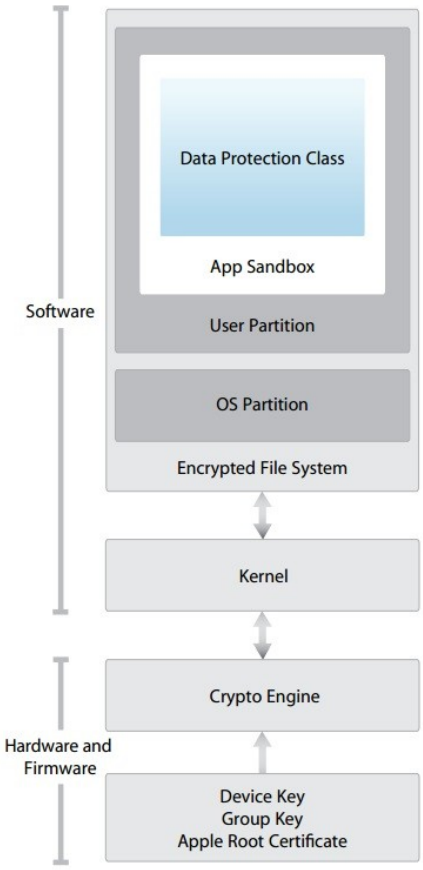
Kromě základních zabezpečovacích mechanismů, jako je např. užití kódového zámku, nabízí iOS i pokročilejší techniky a metody ochrany dat uživatele, které byly integrovány v sedmé verzi, v níž bylo zabezpečení výrazně posíleno:

- Touch ID, snímač otisků prstů,
- integrace jednotného přihlášení do korporátních aplikací a služeb,
- zabezpečení spojení konektivity Airdrop (ať už Wi-Fi nebo Bluetooth)
- iCloud Keychain pro generování a správu silných hesel pomocí 256 bitového šifrování AES,
- Secure Enclave, bezpečnostní koprocesor integrovaný do 64bitového procesoru Apple A7 [6],
- a další metody, které umožňují na dálku vymazat obsah zařízení, pokud bylo ztraceno nebo zcizeno.

„Řada profesionálů dosud nepovažovala produkty Apple za dostatečně zralé pro korporátní či státní bezpečnost, ale Apple se možná pomalu stává standardem v mobilní bezpečnosti. Již nyní jsou možná zařízení Apple zabezpečenější než jakékoli jiné běžně dostupné zařízení“, tvrdí bezpečností analytik Rich Mogull[14].

Jedinou oficiální cestou, jak instalovat aplikace do zařízení s iOS je prostřednictvím oficiální distribuční služby App Store. Vzhledem k přísným kontrolám obsahu této služby není možné, aby si uživatel nainstaloval aplikaci se škodlivým kódem a společnost Apple Inc. proto tvrdí, že nemá význam používat antivirové programy. Pokud je ale zařízení se systémem iOS softwarově upraveno pomocí tzv. jailbreaku, který umožňuje částečně systém otevřít a je tedy možné upravovat systémové soubory, instalovat aplikace pocházející z neoficiálních zdrojů atp., pak se naskýtá možnost napadení zařízení případným útočníkem. Za to již ale Apple odmítá zodpovědnost.

Na obrázku níže je graficky zobrazena bezpečnostní architektura systému iOS, kde je patrné složení bezpečnostní architektury ze dvou částí.



Obr. 2.3.2 – Bezpečnostní architektura systému iOS

[zdroj: http://www.macobserver.com/imgs/tmo_articles/20120604iossecurityguide1.jpg]

Softwarová část:

- Kernel (jádro) po svém startu při zapnutí přístroje ověří, které procesy a aplikace smí být spuštěny. Aby bylo zajištěno spuštění pouze důvěryhodných aplikací, musí být kód zkontrolován a obsahovat certifikát společnosti Apple.
- Šifrovaný souborový systém (Encrypted File System) komunikuje s jádrem systému (Kernel) a skládá se ze dvou částí:
    - OS Partition (Oddíl operačního systému) - je určen pouze pro čtení a nacházejí se zde předinstalované aplikace a systémové soubory,
    - User Partition (Uživatelský oddíl) – zde jsou instalovány aplikace třetích stran. Aplikace zde spuštěná se nachází v tzv. sandboxu, který zamezuje přímému čtení a úpravě dat či programové logiky jiných aplikací. Pokud je ale vyžadován přístup k těmto informacím, činí tak prostřednictvím aplikačního rozhraní a služeb poskytovaných iOS. Po instalaci každé aplikace je vytvořena s ní svázána třída Data Protection Class obsahující bezpečnostní politiku a řízení přístupu k datům dané aplikace.

Hardwarová a firmwarová část:

- Crypto Engine – obstarává AES šifrování a je implementován přímo v hardwarovém vybavení zařízení[6],
- Device Key – šifrování zařízení, uživateli není umožněno ho konfigurovat,
- Group Key – sdílené šifrování mezi aplikacemi, umožňuje sdílet určitá data,
- Apple Root Certificate – předinstalovaný certifikát ověřující jiné certifikáty z důvěryhodných zdrojů.

2.4 Windows Phone

Obr. 2.4.1 - Logo Windows Phone

[zdroj:http://cmsresources.windowsphone.com/windowsphone/shared/WindowsPhone-68217A-175x25.png]

Mobilní operační systém Windows Phone určený pro mobilní telefony je nástupcem systému Windows Mobile, který byl zmíněn v kapitole 2.1. Jeho historie se datuje od roku 2010 a hlavním poznávacím znakem je uživatelské rozhraní Metro složené z tzv. dlaždic, které slouží jako odkazy na jednotlivé aplikace, funkce, mediální položky a kontakty uložené v zařízení. Velmi podobné rozhraní se stejným označením se nachází i v desktopovém

operačním systému Windows 8, který bývá v odlehčené verzi pod názvem Windows RT využíván na mobilních zařízeních a to konkrétně na tabletech. Některé z těchto tabletů disponují funkcí dual-boot, která dává možnost uživateli si vybrat, který operační systém chce spustit – Windows 8 nebo Android. Nejnovější verze systému nese označení Windows Phone 8 a je zpětně nekompatibilní se systémem Windows Phone 7, což je následkem použití nového jádra z řady Windows NT. Podobně jako mobilní operační systém společnosti Apple, iOS, je Windows Phone uzavřeným operačním systémem, uživateli tedy není umožněno zasahovat do systémových souborů.

Domovská obrazovka představuje hlavní plochu uživatelského rozhraní. Dlaždice, které se zde nacházejí, jsou neustále aktualizovány a přinášejí tak aktuální informace o počasí, aktuální zprávy ze světa nebo upozorňují na nový e-mail. Jejich počet, vzhled i umístění si může uživatel nastavit dle libosti. Podobně jako konkurenční mobilní operační systémy i Windows Phone nabízí svému uživateli přehrávání multimediálních souborů, přístup k internetové síti, pořizování fotografií a videí, atp. Aplikace a jiný obsah lze stáhnout do zařízení prostřednictvím oficiální distribuční služby Windows Phone Store.

2.4.1 Zabezpečení

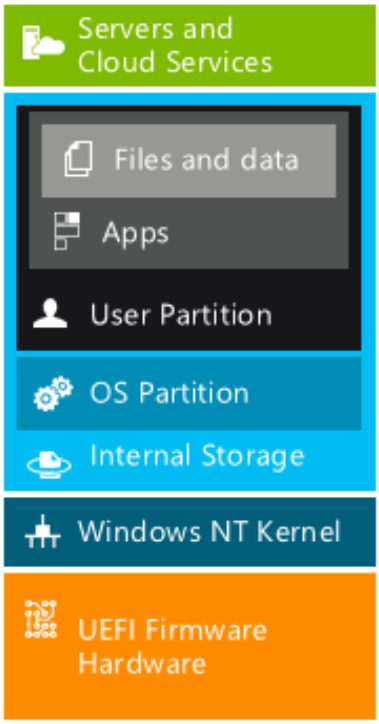
Jak již bylo napsáno výše, Windows Phone 8 se od svého předchůdce, Windows Phone 7, liší použitým jádrem systému, s čímž souvisí i jiný způsob zabezpečení. Vzhledem k tomu, že verze 8 je verzí aktuální, bude se tato podkapitola zabývat výhradně bezpečnostním modelem této verze.

Pro ochranu dat je v mobilním operačním systému Windows Phone implantována řada mechanismů. Tím nejzákladnějším je i zde kódový zámek, který spočívá v nastavení číselného hesla, neboli PIN kódu, a při každém obnovení zařízení režimu spánku je nutno tento kód zadat na tzv. zamykací obrazovce. V opačném případě nebude uživateli umožněno zobrazit obsah zařízení. K dalším mechanismům patří:

- šifrování nástrojem BitLocker – umožňuje šifrovat veškerý obsah zařízení, od dokumentů po hesla šifrováním operačního systému a datových souborů,
- izolování aplikací – zabraňuje, obdobně jako je tomu u operačního systému iOS, aplikacím získat neoprávněný přístup k datům,

- Microsoft certifikát – slouží k podepsání kódu, který je zkontrolován a pochází z důvěryhodného zdroje. Jsou tak spuštěny pouze ověřené softwarové součásti,
- správa přístupových práv.

Bezpečnostní architektura Windows Phone 8 je založena na modelu bezpečného prostředí aplikací výrobců třetích stran. Každá z těchto aplikací přistupuje pouze k izolované paměti a nemůže číst ani zapisovat do sdílených dat systému.



Obr. 2.4.2 - Bezpečnostní architektura Windows Phone 8

[zdroj: MICROSOFT CORPORATION. *Windows Phone 8 Security Guide* [pdf]. 2013 [cit. 14.3.2014]. Dostupné z: http://www.microsoft.com/en-us/download/details.aspx?id=36173]

Na obrázku 2.4.2 je znázorněna bezpečnostní architektura Windows Phone 8. Je zde viditelné rozdělení do čtyř základních částí:

- Servers and Cloud Services (servery a služby cloudu) - Windows Phone 8 podporuje nejnovější verzi EAS protokolu pro bezpečný a stabilní přenos dat služeb, jako jsou např.: Exchange Server, SharePoint, a cloudových služeb jako je Office 365, Windows Intune a Windows Azure, které jsou provozovány na serveru zprostředkovatele. Kromě šifrování mohou správci služeb využít možnosti přidělení přístupových práv k jednotlivým souborům.

- Internal Storage (interní úložiště) obsahuje data, které lze podle obsahu a účelu rozdělit na dvě části:
    - OS Partition (Oddíl operačního systému) - obsahuje předinstalované aplikace a systémové soubory Windows Phone 8,
    - User Partition (Uživatelský oddíl).
        - Apps (aplikace) – zde se nacházejí aplikace třetích stran (a také izolovaná paměť obsahující soubory a data dané aplikace)
- Windows NT Kernel – jádro systému Windows NT.
- UEFI Firmware, Hardware – Bezpečnostní architektura Windows Phone 8 využívá tzv. UEFI, standardní rozhraní firmwaru počítače, vestavěné již při výrobě. Zjednodušeně lze označit jako prostředník mezi použitým hardwarovým vybavením a operačním systémem. V okamžiku vyslání zapínacího signálu jsou spuštěny zaváděcí procesy, o jejichž ověření a bezpečnost se stará právě UEFI. Poté je spuštěn boot manager operačního systému, který zajistí dokončení procesu zavádění systému.

Společnost Microsoft na začátku roku 2013 na svých webových stránkách uvedla, že 8. července 2014 ukončí podporu operačního systému Windows Phone 8. Po tomto datu již nebude možné zařízení s tímto systémem aktualizovat.

2.5 Mobilní zařízení

V předchozích kapitolách uvedené operační systémy jsou jednou částí výkonného celku, druhá část je hardwarová, kterou představují mobilní zařízení, z nichž některé již byly zmíněny výše. V této podkapitole je uveden stručný popis těch nejrozšířenějších.

Jako mobilní zařízení jsou obecně označovány bezdrátové přenosné elektronické přístroje disponující vlastním napájením a operačním systémem, který umožňuje spuštění aplikací.

- Smartphone, česky označovaný rovněž jako chytrý telefon, je mobilní telefon využívající mobilní operační systém, který umožňuje instalaci aplikací, které nejsou obsaženy v samotném systému. Většina smartphonů obsahuje GPS čip pro navigaci,

přední a zadní kameru pro pořizování fotografií a uskutečňování videohovorů, a vzhledem k rostoucí popularitě hraní her na mobilních zařízeních, obsahují moderní smartphony i výkonné grafické čipy.

- Tablet je přenosný počítač, jehož přední stranu pokrývá dotykový display o velikosti sedmi a více palců. Svým hardwarovým zařízením se moc neliší od smartphonů, některé tablety disponují i slotem na SIM kartu a uživateli je umožněno využívat 3G síť pro připojení k internetu a telefonovat. Někdy jsou tyto tablety označovány jako phablety.
- Netbook lze zjednodušeně popsat jako zmenšený notebook. Jedná se o přenosný počítač s hardwarovou klávesnicí s důrazem na mobilitu, tzn. na nízkou spotřebu, rozměry i váhu. Netbook lze využít k přístupu na internet, jednodušší kancelářské práci a jako multimediální přehrávač.
- Čtečka elektronických knih, ebook nebo také čtečka e-knih, je mobilní zařízení kompaktních rozměrů umožňující na úsporných displayích zobrazit elektronické verze knih. Některé modely umožňují i prohlížení internetového obsahu prostřednictvím Wi-Fi připojení a poslech souborů ve formátu MP3.
- Chytré hodinky mají podobu klasických náramkových hodinek, avšak místo ciferníku se zde nachází malý display. Hodinky běžící na upraveném mobilním operačním systému se pomocí Bluetooth spojí s mobilním telefonem a informují uživatele o zmeškaných hovorech, událostech v kalendáři, a umožňují číst SMS zprávy a e-maily. Dalším zařízením, které může uživatel nosit na ruce, jsou tzv. chytré náramky, které nabízejí podobné funkce jako chytré hodinky ale některé modely navíc přidávají funkci měření srdečního tepu nebo krokoměr a nacházejí tak své využití zejména u sportovně aktivních uživatelů. Výrobci v těchto zařízeních spatřují potenciál využití nejen u sportovců ale také u uživatelů, kteří mají zájem chránit svá data uložená v mobilních zařízeních. Speciálně upravené náramky by měly na základě srdečního rytmu jednoznačně identifikovat uživatele a povolit mu tak přístup k zařízení. První prototyp, Nymi bracelet, je již vyvinut a pokud by došlo k masovému rozšíření, mohlo by to znamenat velký pokrok v zabezpečení dat[7].

3 Analýza bezpečnosti OS Android

Otevřenost systému Android je jedním z faktorů masového rozšíření a popularity. Po zveřejnění většiny zdrojového kódu se mnozí výrobci elektroniky zaměřili právě na tento systém, jehož nasazení do vlastních zařízení jim ušetřil velkou část finančních zdrojů, které by jinak mohly být vynaloženy na vývoj vlastního operačního systému. Někteří výrobci využívají možnosti úpravy kódu a přicházejí tak s vlastním uživatelským rozhraním a nabídkou funkcí či služeb. To však vede ke značné roztříštěnosti verzí systému. Byť vývojáři nabádají k používání nejnovějších verzí systému, v praxi se na trhu vyskytují mnohá zařízení, jejichž použité verze obsahují již odhalené bezpečnostní chyby. Zde jsou však do jisté míry na vině právě výrobci, kteří obstarávají distribuci optimalizačních a bezpečnostních aktualizací. Neustálé rozšiřování portfolia, uvádění nových modelů na trh a náročná optimalizace vedlo k nepsanému pravidlu, kdy bývá ukončená softwarová podpora zařízení přibližně do jednoho roku a půl od uvedení daného zařízení na trh. Na otázku proč Google nezajišťuje veškeré aktualizace, jako to dělá např. společnost Apple, Andy Rubin, vedoucí vývojového týmu, odpověděl, že ovládat veškerá zařízení by bylo skvělé, avšak jedná se o velmi vysoký počet těchto zařízení a pokud by se přesto na tento problém zaměřili, nebylo by možné tak rychle inovovat, zvláště tehdy, když vše pochází od jednoho dodavatele[1]. V tabulce níže je vypsán podíl jednotlivých verzí aktuální k datu 3. březen 2014.

Verze	Označení	Podíl
2.2	Froyo	1.2%
2.3.3 - 2.3.7	Gingerbread	19.0%
3.2	Honeycomb	0.1%
4.0.3 - 4.0.4	Ice Cream Sandwich	15.2%
4.1.x	Jelly Bean	35.3%
4.2.x	Jelly Bean	17.1%
4.3	Jelly Bean	9.6%
4.4	KitKat	2.5%

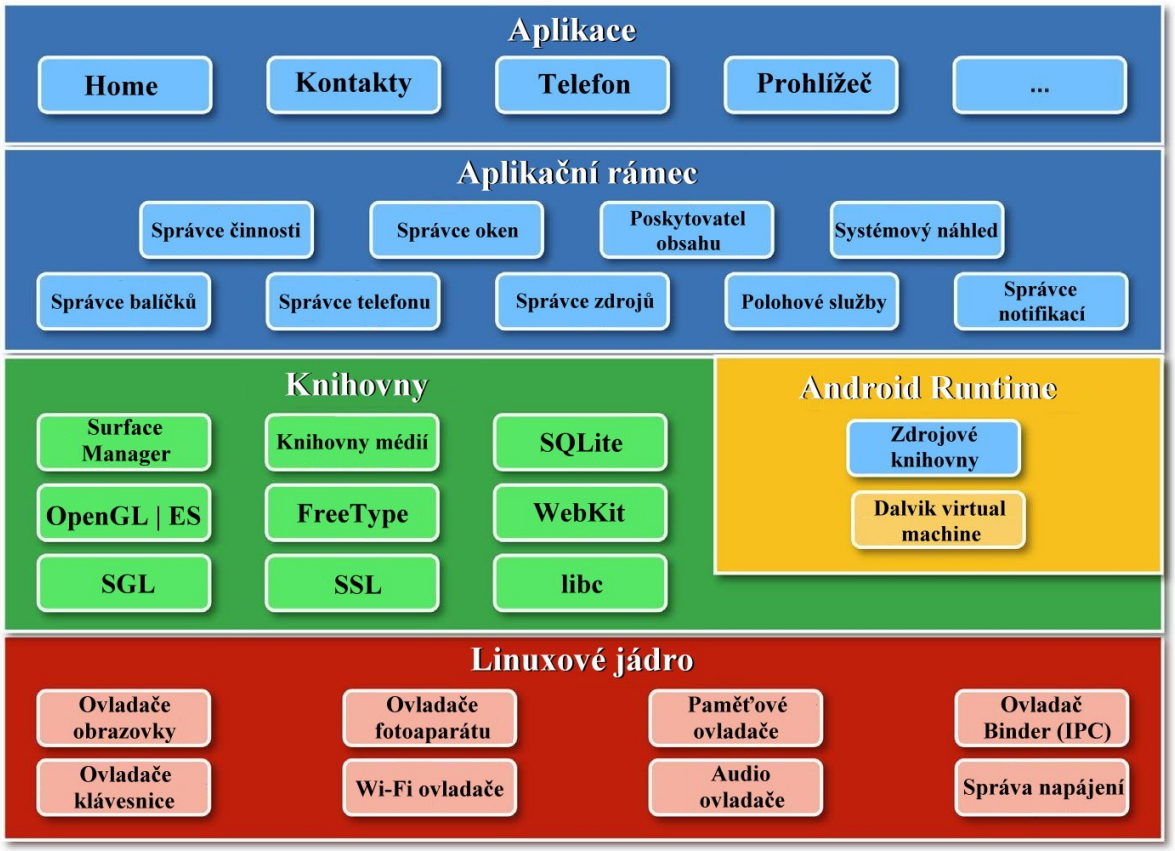
Tabulka 3.1 - Podíl jednotlivých verzí

[zdroj: https://developer.android.com/about/dashboards/index.html#Platform]

Nejrozšířenější verzí je 4.1 Jelly Bean a nejaktuálnější verzi, 4.4 KitKat, obsahuje pouhých 2,5% všech zařízení se systémem Android. Velmi významný podíl zastává i verze 2.3 Gingerbread, která byla uvedena na konci roku 2010 a je tedy neaktuální.

3.1 Architektura OS Android

Jak již bylo zmíněno v kapitole 2.2, operační systém Android je otevřený systém založený na Linuxovém jádře ve verzi 2.6, v nejnovějších verzích systému je využito jádro 3.4. Hardwarová architektura Androidu se odvíjí od specifického typu zařízení, jelikož Android je vyvíjený jako hardwarově nezávislý. Softwarová architektura se skládá z několika vrstev, z nichž každá zodpovídá za určitou činnost systému a je oddělena od vyšších vrstev, kterým poskytuje specifické služby [2]. Rozdělení do vrstev je běžná technika při vývoji složitého softwaru a umožňuje tak rozdělit celek do menších částí.



Obr. 3.1.1 - Architektura OS Android [zdroj: vlastní]

Z grafického vyobrazení na obrázku Obr. 3.1.1 je patrné rozdělení do čtyř vrstev [3]:

- **Linuxové jádro**

  Základem operačního systému Android je Linuxové jádro. To tvoří nejnižší vrstvu architektury, na které probíhá přímá komunikace s příslušným hardwarovým vybavením. Podobně jako na stolních počítačích s operačním systémem Linux, i zde má jádro na starost zavádění systému do operační paměti a správu hardwaru. Při startu zařízení je jádru předáno řízení a má tak kontrolu nad systémem a běžícími procesy. Nízkoúrovňové funkce zahrnují ovladače obrazovky, fotoaparátu, klávesnice, Wi-Fi ovladače, paměťové ovladače, audio ovladače, správu napájení a ovladač Binder, který umožňuje komunikaci mezi procesy a jejich spolupráci.

- **Knihovny, Android Runtime**

  Druhá vrstva zahrnuje řadu knihoven napsaných v programovacím jazyce C/C++ poskytující základní funkce pro vývojáře, kteří k nim přistupují prostřednictvím vyšší vrstvy. Mezi knihovny patří:
  - Surface manager – řídí přístup k subsystému displaye a vytváří tzv. grafické plochy tvořené 2D a 3D grafikou, které se následně na displayi zobrazují [4],
  - knihovny médií – umožňují spouštění a nahrávání multimediálních souborů,
  - SQLite – knihovna obsahující relační databázi, která je dostupná všem aplikacím a tvoří tak základní datové úložiště operačního systému Android,
  - FreeType – knihovna pro bitmapové a vektorové vykreslování písma [5],
  - WebKit – nástroj pro zobrazování webového obsahu prohlížečem,
  - grafické knihovny (OpenGL / ES, SGL) – umožňují přístup k nástrojům určených pro vykreslování 2D a 3D grafiky,
  - SSL – knihovna určená pro podporu využití šifrovacího protokolu pro zajištění bezpečné internetové komunikace,
  - libc – standardní C knihovna optimalizovaná pro Linux na bázi embedded zařízení [5].

Na druhé vrstvě se rovněž nachází komponenta Android Runtime skládající se ze dvou částí:

- Dalvik Virtual Machine je virtuální stroj vyvíjený speciálně pro operační systém Android a tvoří jeho důležitou součást. Jeho úkolem je komunikovat a spouštět aplikace i na zařízeních s nízkým výkonem procesoru, operační pamětí a šetřit energii. Dalvik Virtual Machine úzce souvisí s virtuálním strojem Java Virtual Machine, rozdíl je v architektuře a koncovkách spouštěných souborů. Vývoj Dalviku speciálně pro operační systém Android ovlivnily dva faktory – Java Virtual Machine není volně šiřitelný a virtuální stroj Dalvik je optimalizován pro mobilní zařízení.
- Zdrojové knihovny – poskytují základní funkce jádra programovacího jazyka Java. Nejsou obsaženy knihovny pro práci s uživatelským rozhraním AWT a Swing, které jsou nahrazeny knihovnami pro uživatelské prostředí Android a rovněž přibyly knihovny Apache určené pro práci se sítí.

- **Aplikační rámec**

  Aplikační rámec zahrnuje celou řadu služeb a funkcí, ke kterým vývojáři mohou přistupovat a tvořit tak zajímavé a inovativní aplikace pro uživatele. Prostřednictvím aplikačního rámce mohou přistupovat k hardwarovému vybavení daného zařízení nebo např. využívat prvky graficko-uživatelského rozhraní. Mezi služby patří:

  - správce činnosti (Activity Manager) – řídí životní cyklus aplikací, tj. jejich start, průběh a ukončení,
  - poskytovatel obsahu (Content Providers) – umožňuje přistupovat a pracovat s obsahem jiných aplikací, např. Kalendář, e-mail atp.,
  - systémový náhled (View System) – umožňuje vývojářům při tvorbě graficko-uživatelského rozhraní použít prvky jako textová pole, tlačítka, přepínače, aj.,
  - správce balíčků (Package Manager) – nese informace o aplikacích nainstalovaných do operačního systému,
  - správce zdrojů (Resource Manager) – poskytuje přístup nekódovým zdrojům, jako jsou řetězce, grafika, přidané soubory [5],
  - správce notifikací (Notification Manager) - umožňuje aplikacím zobrazení upozornění ve stavovém řádku grafického rozhraní, a další viz. Obr.3.1.1.

- **Aplikace**

  Na nejvyšší vrstvě se nachází základní aplikace operačního systému Android. Patří zde, např. e-mailový klient, SMS, kalendář, internetový prohlížeč atp. Rovněž jsou zde aplikace, které si uživatel doinstaloval prostřednictvím oficiální distribuční služby Google Play, popř. z paměťové karty. Aplikace jsou programovány v jazyce Java, poté jsou přeloženy do Java byte kódu. Pomocí Dalvik kompilátoru jsou dále přeloženy do mezikódu a výsledný byte kód je spuštěn na Dalvik Virtual Machine jako samostatný proces[5].

3.2 Bezpečnostní model

Mobilní operační systém Android vzhledem k faktu, že se jedná o open-source systém, využívá jiný bezpečnostní model než konkurenční mobilní operační systémy. Pro ochranu dat uživatele jsou v systému implementovány bezpečnostní mechanismy, které jsou popsány níže v této podkapitole. Android byl záměrně navržen tak, aby se snížila zátěž na vývojáře, a ti méně zkušení mohli rovněž vytvářet bezpečné aplikace. Pomyslným srdcem celého systému je Linuxové jádro a tvoří tak i základ bezpečnostního modelu.

3.2.1 Bezpečnostní koncept Linuxového jádra

Koncept bezpečnosti Linuxu je založen na uživatelích a skupinách. Každému uživateli je přiřazeno identifikační číslo, tzv. UID (user identifier), ve chvíli, kdy je profil uživatele vytvořen. Identifikační číslo slouží k odlišení jednotlivých uživatelů, kteří mohou být dále přiřazeni do skupin, které mají vlastní identifikační čísla, tzv. GID (group identifier), pro odlišení skupin uživatelů. Každý uživatel může být členem více skupin a každá skupina může zahrnovat více uživatelů. Na základě identifikačních čísel spojených s daným uživatelem či skupinou a jim přiřazených oprávnění jsou určovány přístupy k souborům. Tato oprávnění jsou přiřazovány vlastníkem souboru. V systému Linux jsou rozlišovány tři sady oprávnění:

- vlastník – práva pro majitele souboru,
- skupina – práva pro určitou skupinu,
- svět – práva pro všechny ostatní uživatele.

Každá sada oprávnění může zahrnovat čtení obsahu souboru, zapisování nebo aktualizaci souboru a spouštění souboru za podmínky, že se jedná o spustitelný kód. Pokud mají členové dané skupiny právo zapisovat do souboru, mají rovněž právo ho i číst. Jestliže nabývají pouze práva číst soubor, pak do něj nemohou zapisovat. Jak vyplývá z výše uvedeného, oprávnění v systému Linux je tedy založeno na jednoduché myšlence. Pokud určitý uživatel nebo skupina uživatelů nemá potřebná práva, nemohou provádět dané úkony, popř. nemají přístup k souboru. Operační systém Android využívá Linuxové jádro a přebírá tak jeho bezpečnostní mechanismy. Pokud uživatel nainstaluje Android balíček, např. aplikaci, hru atp., pak systém zajistí vytvoření nového identifikačního čísla uživatele, které je jedinečné na daném zařízení, a aplikace poté poběží pod tímto UID. Veškerá data této aplikace, např. databáze, soubory, nesou stejné identifikační číslo na základě kterého je rovněž určen plný přístup, tzn. zapisování, aktualizace, čtení a spouštění souborů. Na základě UID jsou odděleny i procesy a přístup k operační paměti při provádění úkolů jednotlivých aplikací. Tento mechanismus karantény, tzv. sandbox, je aplikován na veškeré aplikace i knihovny operačního systému běžící nad vrstvou Linuxového jádra, tzn. nad první vrstvou architektury Androidu [4]. Pokud však vývojář explicitně nakonfiguruje stejné UID u dvou či více aplikací, mohou si tyto aplikace vzájemně přistupovat k souborům a mít nad nimi plnou kontrolu. Přístup k datům všech aplikací má tzv. root UID.

Většina mobilních zařízení nabízí uživateli rozšíření paměti pomocí externích paměťových karet. Na tyto datová úložiště se nevztahuje bezpečnostní mechanismus řízení přístupu a jakýkoliv soubor, který se zde nachází, je tak přístupný všem aplikacím v zařízení. Tato výjimka je důsledkem používaného systému souborů paměťových karet, který nepodporuje standardní systém oprávnění používaný v Linuxu. Pro zabezpečení dat je vhodné využít šifrovací metody.

Pro správnou funkčnost některých aplikací je zapotřebí komunikace mezi oddělenými procesy. Meziprocesová komunikace, IPC, je rovněž bezpečnostně zajištěna na úrovni Linuxového jádra.

3.2.2 Podepisování aplikací

Každá aplikace určená pro mobilní operační systém Android je digitálně podepsaná. Digitální podpis je aplikací asymetrické kryptografie, jehož pomocí prokazuje autor, že skutečně danou aplikaci vytvořil. Zjednodušeně lze digitální podpis přirovnat ke

klasickému vlastnoručnímu podpisu, kterým je prokazována totožnost autora a lze jen stěží tento podpis napodobit. Skládá se ze tří částí:

- Digitální certifikát – identifikuje každého vývojáře, slouží k ověření totožnosti a dělí se na dva typy:
  - certifikáty vytvořené certifikačními autoritami (CA),
  - certifikát vytvořený samotným vývojářem.
- Soukromý klíč – tvořen velmi dlouhým číslem; je podstatné, aby soukromý klíč byl znám pouze jeho vlastníkovi, v opačném případě může být zneužit k vytvoření falešného digitálního podpisu.
- Veřejný klíč – nachází se ve zkompilovaném souboru APK a je určen pro dešifrování odpovědi týkající se stavu licence.

Aplikace musí být podepsány před samotnou instalací na zařízení. Systém Android však nevyžaduje pouze digitálně podepsané aplikace s certifikátem vydaným certifikační autoritou, ale přijme i certifikát podepsaný vývojářem. Aplikace podepsané stejným vývojářem mohou spolu komunikovat na vyšším stupni než s ostatními aplikacemi.

3.2.3 Oprávnění aplikací

Některé aplikace vyžadují pro svou činnost komunikaci a sdílení informací s jinými aplikacemi. Pro ochranu dat má Android implementován systém oprávnění. Ve výchozím nastavení nemá aplikace oprávnění k provádění činností, které by mohly poškodit nebo ovlivnit jiné aplikace na tomtéž zařízení. Rovněž nemůže komunikovat s operačním systémem Android, volat aplikační rozhraní pro používání fotoaparátu, GPS atp., číst a zapisovat data uživatele. Tento úkol je zpracováván na úrovni Linuxového jádra. Seznam požadovaných oprávnění pro správnou funkčnost aplikace je vytvořen vývojářem. Tento seznam se zobrazí při instalaci na daném zařízení ve formě dialogového okna. V tomto bodě přichází na řadu uživatel, který musí explicitně potvrdit souhlas se všemi potřebnými oprávněními, v opačném případě aplikace nebude nainstalována. Zobrazení seznamu uživateli má pomoci varovat před potenciálně nebezpečnými aplikacemi, určit, zda odpovídá potřebám a očekáváním uživatele a rovněž porovnat s alternativními aplikacemi. Některé jiné platformy požadují potvrzení před každým spuštěním aplikací nebo určitých relací.

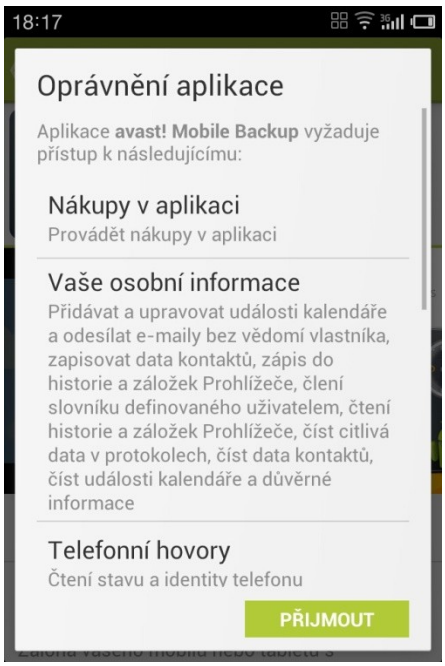
Vývojáři Androidu se však vydali jinou cestou. Jakmile jsou jednou oprávnění přidělena, aplikace jich může využívat do doby, než je odinstalována. V případě opětovné instalace se znovu zobrazí patřičné dialogové okno. Uživatel si může zpětně zobrazit požadovaná oprávnění již instalovaných aplikací prostřednictvím položky Aplikace v nastavení systému.

Z níže uvedeného seznamu lze vyčíst, že některá oprávnění, která mohou být aplikací požadována, umožňují přístup k velmi citlivým datům uživatele. Mezi možná požadovaná oprávnění patří [8]:

- Accounts (účty) – zde spadá vyhledávání a používání uživatelských účtů v zařízení, čtení konfigurace služeb Google,
- Affects battery (ovlivnění spotřeby baterie) – oprávnění přístupu k hardwaru, jehož využití může mít vliv na výdrž baterie,
- Audio Settings (nastavení zvuku) – oprávnění pro přímý přístup k nastavení reproduktorů na daném zařízení,
- Bluetooth Network (síť Bluetooth) – oprávnění pro přístup k jiným zařízením prostřednictvím Bluetooth,
- Calendar (kalendář) – oprávnění přístupu ke kalendáři v zařízení, zobrazení a vytvoření událostí,
- Camera (fotoaparát/kamera) – oprávnění pro užití fotoaparátu/kamery, pořizování snímků a videa,
- Cost money (zpoplatnění) – aplikace vyžadující toto oprávnění může využívat platební kartu uživatele bez jeho přímé účasti,
- Location (umístění, poloha) – oprávnění umožňující zjistit aktuální polohu zařízení prostřednictvím GPS nebo sítě, k níž je zařízení připojeno,
- Messages (zprávy) – po potvrzení oprávnění je aplikaci umožněno číst a odesílat zprávy jménem uživatele,
- Microphone (mikrofon) – oprávnění k využití mikrofonu zařízení,
- Network (sítě) – oprávnění pro přístup k síťovým službám,
- Phone Calls (telefonní hovory) – oprávnění spojeno s přístupem a úpravou seznamu hovorů,
- Social Info (sociální informace) - oprávnění pro přístup k seznamu kontaktů, protokolů volání atd.,

- Storage (úložiště) – oprávnění pro přístup k paměťové kartě,
- Voicemail (hlasová schránka) – oprávnění pro přístup do uživatelovy hlasové schránky.

V souvislosti s oprávněním aplikací byla objevena bezpečnostní trhlina v aktualizačním systému nazvaná pileup. Pokud byla nainstalována aplikace vyžadující oprávnění, které starší verze Androidu ve výchozím stavu nenabízí, aplikace toto oprávnění získá. Po aktualizačním procesu systému na novější verzi přibude nová funkce s novým oprávněním a dříve nainstalovaná aplikace toto oprávnění získá, aniž by byl uživatel dotázán, zda s přidělením souhlasí. Tato situace je důsledkem toho, že systém předpokládá, že oprávnění bylo uživatelem uděleno dříve a není tedy nutné o něj znovu žádat. Aplikace tak může ovlivňovat zobrazovaný obsah webových stránek či sbírat osobní údaje[9].



Obr. 3.2.1 - Příklad požadovaných oprávnění při instalaci aplikace [zdroj: vlastní]

Mezi další součásti bezpečnostního modelu patří:

- Zabránění přístupu k SIM kartě aplikacím třetích stran. Veškerou komunikaci se SIM kartou obstarává operační systém a to včetně přístupu k osobním informacím jako jsou kontakty v její paměti.
- Některé aplikace vyžadují oprávnění pro přístup k umístění uživatele. Po instalaci při prvním spuštění se zobrazí uživateli dotaz, zda chce povolit

aplikaci přístup k jeho poloze. Pokud bude požadavek zamítnut, aplikace nemusí pracovat správně. Toto se může týkat např. navigačních programů atp. Uživatel může zakázat přístup k jeho poloze i prostřednictvím nastavení, kde zruší povolení satelitů GPS a použití bezdrátových sítí.

- Operační systém Android obsahuje ve verzi 4.2 a novější mechanismus ověřování aplikací, který má zabránit instalaci škodlivého softwaru do zařízení. Pokud se uživatel se zapnutým ověřováním pokusí nainstalovat aplikaci z libovolného zdroje, odešle dané zařízení do Googlu informace, na základě kterých bude tato aplikace identifikována. V případě, že se jedná o škodlivou aplikaci, Google zpětně uživatele upozorní, aby ji neinstaloval, popř. instalaci zcela zablokuje.
- Důležitou součástí bezpečnostního modelu Androidu je rovněž systém aktualizací systému. Existují dva základní způsoby distribuce aktualizací: over-the-air, tj. prostřednictvím internetu přímo v daném zařízení a pomocí souborů zip, které si uživatel stáhne z příslušných zdrojů na paměťovou kartu do svého zařízení. Jakmile Android tuto aktualizaci rozpozná, ověří jeho autenticitu a integritu a automaticky aktualizuje systém v zařízení.

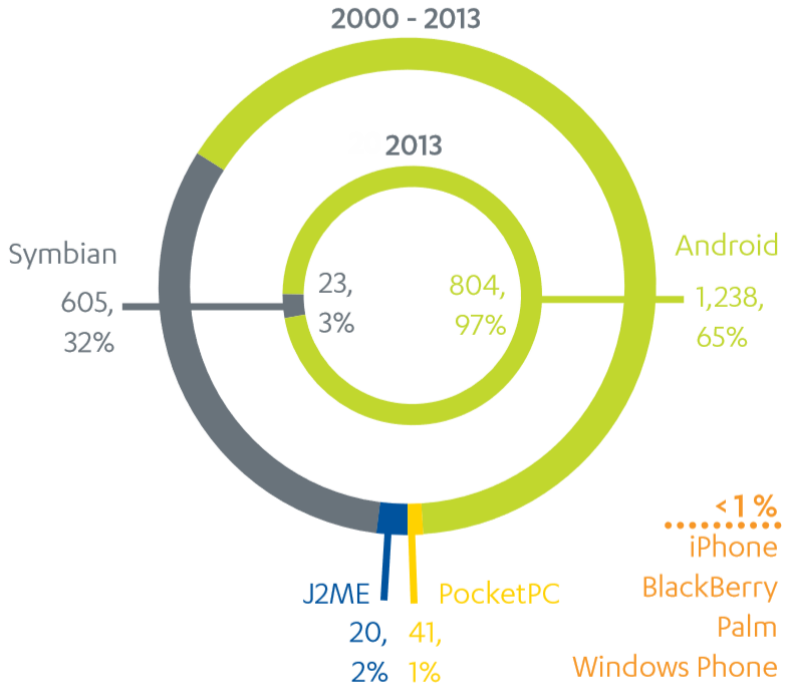
3.3 Škodlivý software pro platformu Android

I přesto, že, jak je z předchozí kapitoly zřejmé, Android užívá velmi sofistikovaný a ucelený bezpečnostní mechanismus, stále jsou objevovány nové trhliny a slabá místa systému. Podobně, jako tomu je u desktopových operačních systémů, i mobilní zařízení začaly být napadány škodlivým softwarem. Mobilní operační systém Android je nejrozšířenějším systémem na světě a mnozí uživatelé mají na mobilních zařízeních velké množství informací osobních i firemních, což z nich činí ideální cíle mnoha útočníků, kteří tak záměrně využívají konkrétních nedostatků v systému. Současná podoba útoků se z hlediska účelu a technického provedení přiblížila těm, které jsou známé z klasických stolních počítačů.

V únoru roku 2014 uvedla společnost Kaspersky Lab, která se řadí mezi nejrychleji rostoucí prodejce v oblasti zabezpečení IT na světě, krátkou tiskovou zprávu, ve které uvádí: „*Ke konci ledna 2014 identifikovala společnost Kaspersky Lab na 200 tisíc jedinečných*

vzorků mobilního malwaru. To je o 34 % víc než v listopadu 2013, kdy odhalila 148 tisíc vzorků. Kybernetičtí zločinci se stále zaměřují hlavně na Android. V lednu tak počet škodlivých aplikací pro Android překročil hranici deseti milionů.“[10]

Vzhledem k faktu, že ke stejnému datu nabízel oficiální obchod Google Play 1 103 104 aplikací, je číslo uvádějící počet škodlivých aplikací pocházejících z neoficiálních obchodů a různých nelegálních zdrojů alarmující. Obchody třetích stran nabízející aplikace, např. Anzhi.com, patří k nejčastěji využívanému distribučnímu kanálu škodlivého softwaru. Běžnou praktikou je tzv. přebalení instalačního balíčku. Tvůrci škodlivé aplikace využívají zájmu o konkrétní aplikace, stáhnou její instalační balíček, např. z oficiálního obchodu Google Play, a přidají do kódu vlastní škodlivé funkce. Poté je aplikace znovu zabalena do instalačního balíčku a uvolněna ke stažení na distribučních kanálech [11].



Obr. 3.2.2 – Podíl škodlivého SW mezi jednotlivými mobilními operačními systémy [11]

Na obrázku výše je graficky znázorněn vývoj rozšíření škodlivého softwaru na mobilních platformách. V letech 2000 až 2013 zde měl ještě významný podíl škodlivý software určený pro mobilní operační systém Symbian, avšak od roku 2013 jasně dominuje Android. Pouze necelé jedno procento zastupuje škodlivý software určený pro mobilní operační systémy iOS, Windows Phone a další. V následujících podkapitolách jsou rozepsány jednotlivé podoby škodlivého softwaru a jejich rozšíření na platformě Android.

3.3.1 Malware

Malware je definován jako jakýkoliv kus škodlivého softwaru, který se nachází na počítači, popř. mobilním zařízení uživatele a jeho úkolem je zničení dat, krádež osobních informací nebo dosažení přístupu k systémovým zdrojům za účelem získání plné kontroly nad daným zařízením [3]. Malware je souhrnným označením počítačových virů, spywaru a trojských koní, avšak přesný obsah pojmu malware na mobilních zařízeních nebyl dosud vymezen. Tento software je vytvořen tak, aby kopíroval sám sebe a rozšířil se i na jiná zařízení.

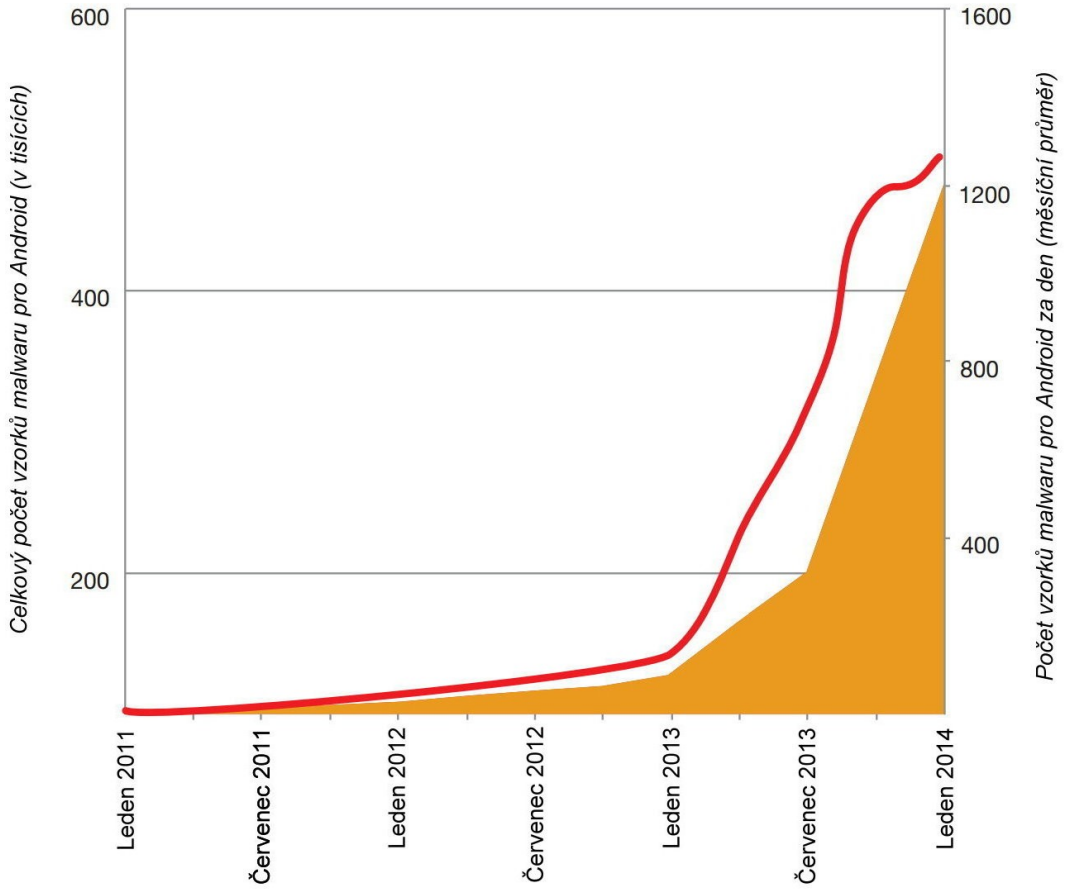
Poprvé byl malware na Androidí platformě spatřen v srpnu 2010. Od té doby byl zaznamenán vysoký nárůst malware rodin. Pojmem malware rodiny jsou označovány skupiny škodlivých softwarů, které sdílejí určité vlastnosti. Od svého prvního výskytu prošel malware značnou obměnou a dokáže se sofistikovaně skrýt před detekčními metodami a následným odstraněním. Útočníci obvykle vyvíjejí nové verze s cílem zjišťování nových bezpečnostních trhlin a přidáváním škodlivých funkcí v reakci na aktualizace systému a antivirů či jiných ochranných nástrojů.

Jako konkrétní příklad může posloužit malware Ginmaster, který byl objeven v srpnu 2011 v Číně a nakazil mnoho legitimních aplikací nacházejících se v obchodech s aplikacemi třetích stran. V roce 2012 začal odolávat detekci pomocí zamlžování jmen tříd, šifrování URL adres a dalšími metodami, které jsou užívány především malwarovými programy určenými pro operační systém Windows.

Již zmíněná společnost Kaspersky Lab objevila na počátku roku 2013 malware, který se výrazně odlišuje velkým počtem škodlivých funkcí. Vývojáři využili poptávky uživatelů po aplikacích, které pomocí ukončení určitých procesů uvolní místo v operační paměti a urychlí tak chod zařízení, a umístili na oficiální obchod s aplikacemi, Google Play, malware, který se maskoval právě jako tento typ aplikace. Na dané stránce obchodu bylo zobrazeno pozitivní hodnocení a vypadala tedy důvěryhodně. Po instalaci a spuštění aplikace se spustilo několik procesů, mezi které patří vymazání a zasílání, tzv. prémiových, SMS zpráv bez vědomí uživatele. Prémiové SMS jsou zpoplatněné zprávy a pokud jsou pod kontrolu útočníka, pak dokážou během několika málo minut vytvořit útratu v řádech tisíců korun. Mezi další procesy spuštěné malwarem patří zapínání Wi-Fi připojení, získávání informací o zařízení, otevření libovolné stránky v prohlížeči, nahrání veškerého obsahu paměťové karty, SMS zpráv, kontaktů, fotografií a polohy zařízení na server určený útočníkem. Již tak značně dlouhý

seznam škodlivých funkcí byl doplněn o jednu, kterou se tento škodlivý software odlišuje od ostatních. Při připojení zařízení k počítači se systémem Windows v režimu „USB úložiště“, který umožňuje kopírování dat do počítače nebo naopak z počítače do zařízení, byl automaticky spuštěn soubor svchosts.exe v němž se nacházel škodlivý kód a převzal kontrolu nad mikrofonem. Nahrané záznamy jsou zašifrovány a odeslány na server útočníka. Zde je nutno poznamenat, že současné verze systému Windows mají ve výchozím nastavení zakázanou funkci AutoRun, automatické spuštění, pro externí disky. Nelze však předpokládat, že všichni uživatelé tyto verze systému používají.

Na grafu níže je zobrazen vývoj růstu malwaru pro operační systém Android za poslední tři roky. V roce 2013 lze pozorovat strmý nárůst zachycených vzorků a předpokládá se, že tento trend bude v roce 2014 pokračovat. Veškerá data jsou sesbírána výzkumným oddělením společnosti Fortinet, FortiGuard Labs. Jedná se však pouze o část skutečného počtu malwarových aplikací a vzhledem k faktu, že společnosti zabývající se touto problematikou provádí vlastní výzkum a sběr informací, prakticky nelze zjistit celkový počet.



Graf 3.1.3 – Růst počtu vzorků malwaru pro Android [12]

3.3.2 Trojský kůň

Trojský kůň je definován jako uživateli skrytá část programu s funkcí, se kterou uživatel nesouhlasí. Trojský kůň určený pro systém Android může mít podobu užitečné aplikace nebo hry aby nalákal případné oběti ke stažení a instalaci.

Největší růst byl zaznamenán u rodiny TrojanSMS.Agent. První verze vznikla v roce 2011 a již o dva roky později, v roce 2013, bylo zjištěno 324 verzí tohoto trojského koně [13].

Nejsofistikovanějším trojským koněm určeným pro operační systém Android je Obad Trojan. Tento škodlivý software může být zmanipulován třetí osobou prostřednictvím SMS, následně nainstalovat do zařízení další škodlivé aplikace a odcizit uživatelovy osobní informace. Šíření je zajištěno pomocí druhého mobilního trojského koně, který lze být, vzhledem ke své funkci, stejně tak považován za botnet, SMS.AndroidOS.Opfake.a, se kterým je distribuován. Opfake.a využije po instalaci Google Cloud Messaging a doručí uživateli zprávu o přijetí MMS zprávy, kterou si může stáhnout z příslušné webové adresy. Pokud uživatel na daný odkaz klikne, bude mu do zařízení nahrán speciální soubor, který po spuštění dostane od kontrolního serveru pokyn k rozeslání stejné zprávy všem kontaktům uživatele. Tato metoda se používá u relativně nízkého počtu škodlivého programů, ale některé z nich jsou velmi rozšířené. Zasílání zpráv Google Cloud Messaging probíhá pomocí Google Cloud Messagin systému a je nemožné je zablokovat přímo na infikovaném zařízení.

Na začátku roku 2014 byl v Číně objeven trojský kůň, který je specifický svým umístěním do chráněné oblasti paměti daného zařízení a spouštěním se ve fázi zavádění operačního systému po zapnutí zařízení. I přesto, že některé jeho části byly odstraněny, alespoň jedna komponenta vždy zůstala v paměti a po restartu znovu infikovala systém. Trojský kůň dostal pojmenování Android.Oldboot.1 a je označován za první bootkit pro Android. Bootkit je škodlivý software, který infikuje spouštěcí kód systému, aby mohl napadnout i šifrované systémové soubory a minimalizoval tak možnost, že bude odstraněn bez zásahu do systému. Android.Oldboot.1 je nainstalován jako typická aplikace, která slouží jako systémová služba a připojuje se ke vzdálenému serveru, odkud přijímá různé příkazy, např. stáhnout, nainstalovat či vymazat určité aplikace.

Trojské koně lze rozdělit do 4 kategorií:

- Downloader Trojan – hledá na internetu další škodlivý software a následně jej instaluje do zařízení,

- Dropper Trojan – postupně instaluje další škodlivý kód, který obsahuje,
- Clicker Trojan – přesměruje uživatele na webové stránky nebo reklamy za účelem většího počtu kliknutí na danou reklamu a tak generuje útočníkovi zisk,
- Bank Trojan – jeho úkolem je zachytit přihlašovací údaje pro online bankovnictví, např. mobilní verze trojského koně Caberp pocházejícího z Ruska zachytává informace uživatelů ve chvíli, kdy jsou odesílány na bankovní server.

3.3.3 Spyware

Spyware je dalším typem škodlivého softwaru, který přistupuje k osobním informacím a následně je z daného zařízení extrahuje. Cílem jsou e-mailové zprávy uživatele,SMS zprávy, seznam kontaktů, fotografie atd. Zaměřit se může rovněž na unikátní identifikátory jako je unikátní výrobní číslo SIM karty ICCID, unikátní číslo přidělené výrobcem daného zařízení, IMEI, a IMSI, unikátní číslo přidělené mobilním operátorem pro danou SIM kartu za účelem dohledávání detailů o uživateli. Dále to může být telefonní číslo, verze přístroje a název síťového operátora. Spyware je vývojáři navržen tak, aby neprováděl žádnou rušivou činnost v zařízení a uživatel si nebyl vědom ztráty svých dat. Šířit se může např. prostřednictvím SMS zprávy, která obsahuje webovou adresu, na niž je umístěn škodlivý kód, který se automaticky stáhne do zařízení. Po nakažení se šíří dále možnostmi, které mu dané zařízení nabízí. Může to být opět prostřednictvím SMS zpráv, e-mailovými zprávami nebo pomocí chatovací aplikace atp.

V roce 2014 byl odhalen nový spyware s názvem Dendroid, který se dokáže maskovat i před automatickou anti-malware kontrolou oficiální distribuční sítě aplikací Google Play. Po nainstalování do zařízení umožní útočníkovi neomezeně přistupovat k fotografiím, zprávám v zařízení, procházet historii navštívených webových stránek a zobrazit informace o účtu na sociální síti Facebook. Dále poskytuje plný přístup ke kameře a mikrofonu, což umožňuje útočníkovi odposlouchávání a nahrávání hovorů oběti.

3.3.4 Botnet

Termín botnet se skládá ze dvou částí – bot a net. Bot je zkratka pro robota. Útočník prostřednictvím škodlivého softwaru může proměnit napadené zařízení do určité podoby robota, který provádí automatizované úlohy přes internet, bez vědomí uživatele. Net lze do

češtiny přeložit jako síť. Cílem útočníků je obvykle infikovat velké množství počítačů, vytvořit z nich boty, a tak vznikne síť – botnet.

Mobilní botnety nabízí ve srovnání s tradičními botnety významné výhody pro útočníka. Mobilní zařízení, zejména smartphony, jsou vypínány svými uživateli jen zřídka a botnety jsou tak vždy k dispozici a připraveny pro nové instrukce. Mezi jejich běžné úkoly patří hromadné zasílání nevyžádané pošty, tzv. spamu, DDoS útoky, které pomocí zahlcení požadavky vyřadí z provozu internetové služby nebo stránky, a špionáž osobních údajů. Vzhledem k nenáročnosti těchto procesů a vysokému výpočetnímu výkonu, který moderní mobilní zařízení nabízejí, nestojí útočníkům takřka nic v cestě.

MTK botnet, který se objevil na začátku roku 2013, a Opfake zmíněný výše dokazují, že mobilní botnety se staly nástrojem pro hlavní cíl kyberzločinců – finanční zisk.

V prosinci 2013 byla objevena do té doby největší síť botů. Botnet s názvem MisoSMS měl za úkol krást textové zprávy a prostřednictvím e-mailu je zasílat útočníkům do Číny. Tento škodlivý software se maskuje jako aplikace na nastavení systému Android.

3.3.5 Ransomware

Ransomware existuje v různých formách již přes dvacet let a je známý zejména ze stolních počítačů. Tento program je určitým druhem malwaru, specifický šifrováním souborů na pevném disku nebo znepřístupněním napadeného zařízení uživateli. Útočník pak požaduje výkupné za opětovné odemknutí. V roce 2013 byl ransomware poprvé spatřen na zařízeních s operačním systémem Android maskovaný jako antivirová aplikace nazvaná Android Defender Platinum. Po spuštění zobrazí varování o napadení malwarem, poté ukončí určité klíčové procesy a odstraní značnou část souborů ve snaze zabránit oběti od obnovení zařízení ze zálohy. Následně je uživateli zobrazena zamykací obrazovka, kde jedinou možností je zaplatit útočníkovi 99.99 dolarů prostřednictvím kreditní karty za plnou verzi tohoto falešného antivirového programu. I přesto, že je tato částka uhrazena, nic se nestane a jediná možnost je kompletně vymazat veškerá data v daném zařízení [12].

3.4 Průzkum informovanosti uživatelů o bezpečnosti OS Android

Jak z předchozích podkapitol vyplývá, riziko nakažení mobilního zařízení a ztráta cenných dat je reálným problémem, který může postihnout každého uživatele. Otázkou je, jakým způsobem k této problematice uživatelé přistupují, zda jsou si vědomi hodnoty uložených dat a podnikají základní kroky k jejich ochraně.

Společnost iScan Online, Inc., která je poskytovatelem bezpečnostních řešení, zveřejnila v listopadu 2013 zprávu s výsledky šetření zabezpečení mobilních zařízení. Ve zprávě bylo uvedeno, že 98% zařízení s operačním systémem Android obsahovalo zranitelný prohlížeč nebo aplikaci společnosti Adobe, jejichž prostřednictvím by mohlo být zařízení napadeno škodlivým softwarem. Jiné společnosti z oboru bezpečnosti v IT se zmiňují ve svých reportech a publikacích o nezodpovědném přístupu uživatelů k instalaci aplikací, kteří potvrzují veškerá požadovaná oprávnění, aniž by si je přečetli a porozuměli jim[1].

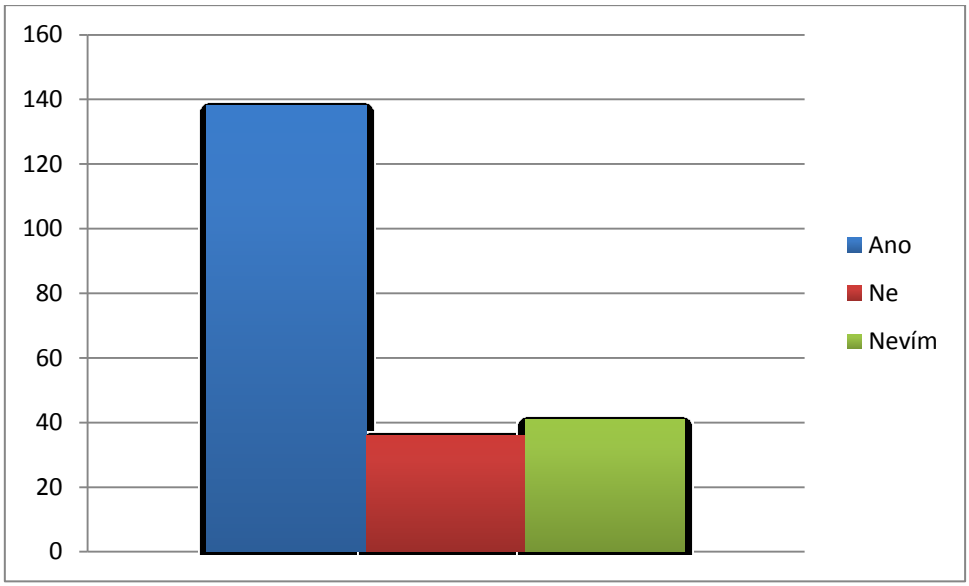
Součástí této diplomové práce je také vlastní průzkum informovanosti uživatelů o bezpečnosti operačního systému Android prostřednictvím dotazníku. Dotazníkové šetření bylo realizováno v elektronické podobě prostřednictvím internetu a tištěnou formou v období od 10. ledna 2014 do 6. dubna 2014. K datu ukončení dotazníkového šetření bylo k dispozici 214 zodpovězených dotazníků, které byly nadále zpracovány pomocí statistických nástrojů Microsoft Excel a Google Docs. Veškeré grafy pocházejí z vlastních zdrojů.

3.4.1 Struktura a vyhodnocení dotazníku

První část dotazníku sloužila k získání přehledu o vzorku respondentů. V další části byli respondenti tázáni, zda se někdy zajímali o danou problematiku na mobilních zařízeních. Rovných 140, 65%, respondentů odpovědělo kladně. Pro přehlednost jsou následující otázky uváděny v plném znění:

- **Existují podle vašeho názoru nějaké hrozby pro běžné uživatele, kteří nijak nezasahují do samotného operačního systému (např. nemají proveden root* na svém zařízení)?**

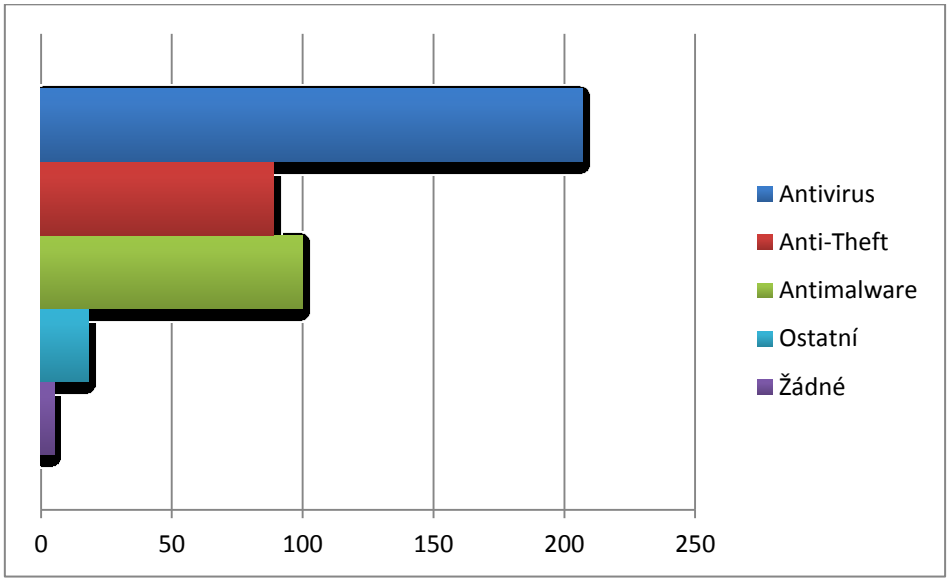
  Pojem root byl respondentům vysvětlen v dotazníku v poznámce pod čarou.



Graf 3.4.1 – Souhrn odpovědí čtvrté otázky [zdroj: vlastní]

Na čtvrtou otázku odpovědělo 64% respondentů kladně, 17% záporně a 19% respondentů zvolilo možnost nevím. Zmíněný termín root označuje systémového superuživatele, který má nejvyšší možné oprávnění. Ekvivalentem může být administrátorský účet známý z operačních systémů pro stolní počítače. Ve výchozím nastavení mobilních zařízení předních světových výrobců mají uživatelé určitá práva odepřena, aby bylo zamezeno poškození systému v důsledku neodborné manipulace se systémovými soubory. Odemčení administrátorských práv, tzv. root, může přinést určité výhody v podobě lepšího zabezpečení proti krádeži pomocí Anti-theft aplikací, možnosti vytvoření plné zálohy všech dat v daném zařízení a odstranění předinstalovaných aplikací, které nelze smazat tradičním způsobem. Mezi nevýhody se řadí větší zranitelnost systému. Méně zkušený uživatel může přidělit jakékoliv aplikaci nejvyšší oprávnění, která mohou být zneužita za účelem krádeže dat. S tvrzením, že běžným uživatelům nezasahujícím do systému nehrozí ztráta dat, odposlouchávání atp., se ztotožnilo 36 odpovídajících, což činí 17% všech respondentů. Takto nízké číslo tvoří zajímavý kontrast s výsledky následujících otázek.

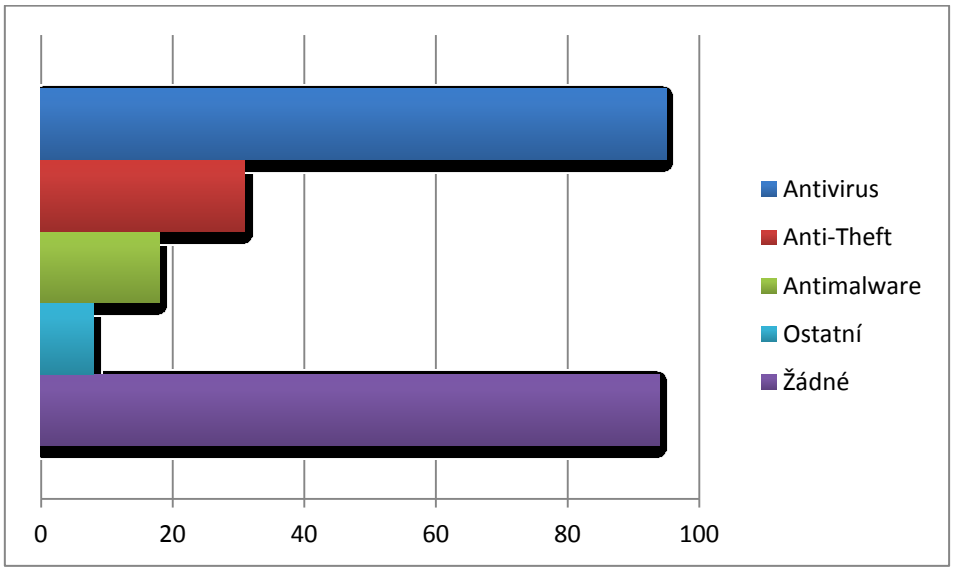
- **Jaké obranné mechanismy znáte (můžete označit více možností)?**



Graf 3.4.2 – Souhrn odpovědí páté otázky [zdroj: vlastní]

V odpovědích jednoznačně převažuje první možnost – antivirus, která byla vybrána 97,7%, tj. 207 respondentů. Jedná se o poměrně vysoké číslo, vzhledem k faktu, že celkový počet respondentů byl 214. Žádné mechanismy dle výsledku šetření nezná pouhé 1% dotazovaných. Respondentům byla rovněž dána možnost, aby sami doplnili další zabezpečovací mechanismy, které jsou jim známy. Tyto odpovědi spadají do položky ostatní a vyskytlo se zde např. zálohování dat a zamykání zařízení pomocí gesta nebo číselného kódu.

- **Jaké obranné mechanismy používáte (můžete označit více možností)?**



Graf 3.4.3 – Souhrn odpovědí šesté otázky [vlastní: zdroj]

Vyhodnocení šesté otázky přináší v porovnání s otázkou předchozí zajímavé výsledky. I přesto, že jsou antivirové aplikace známy více než 96,7% všech respondentů, využívá je pouze 44,4% z nich, což je 95 odpovídajících. Žádné mechanismy pro ochranu dat nevyužívá 94 respondentů a svými 43,9% tak tvoří významný podíl. Při pohledu na výsledky vyhodnocení předchozí otázky se tak jedná o překvapivý kontrast, který je ještě umocněn výsledkem třetí otázky, podle kterého se o problematiku bezpečnosti na mobilních zařízeních zajímalo nebo aktivně zajímá 65% dotazovaných. Nabízí se otázka, proč i přes poměrně rozšířené povědomí o nástrojích ochrany dat nejsou využívány značným počtem respondentů.

- **Zálohujete v pravidelných intervalech svá data (kontakty, SMS zprávy, kalendář aj.)?**

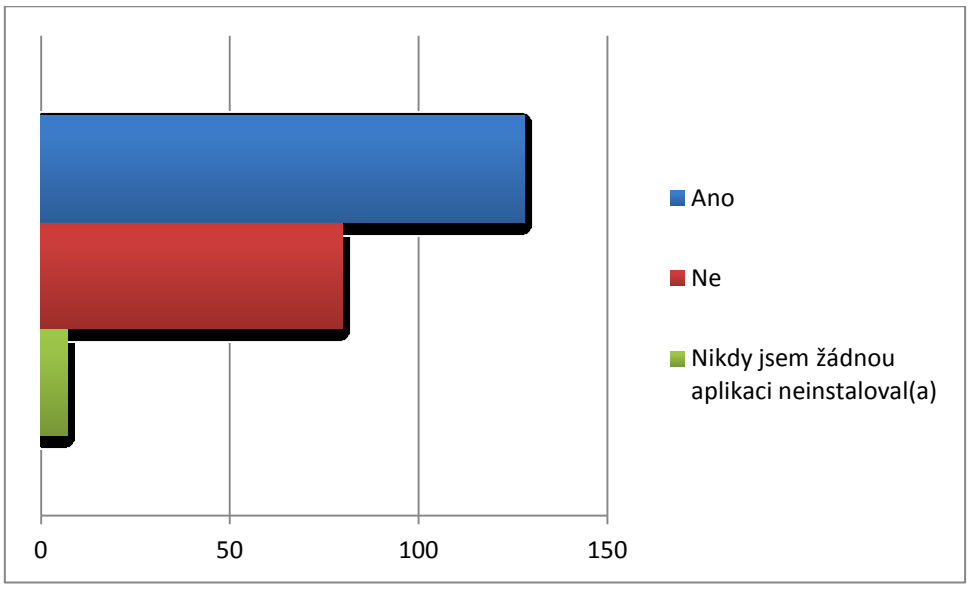
  V pořadí sedmá otázka se týkala záloh uživatelových dat - 49% respondentů odpovědělo, že provádí pravidelné zálohy, 51% odpovědělo, že nikoliv.

- **Přišel/přišla jste již někdy o svá data (kontakty, SMS zprávy, kalendář aj.)?**

  Tato otázka nepřímo navazovala na otázku předchozí. Ztrátu dat potvrdilo 43% dotazovaných, zbývajících 57% o svá data nepřišlo.

- **Čtete si potřebná oprávnění pro běh aplikace při její instalaci?**

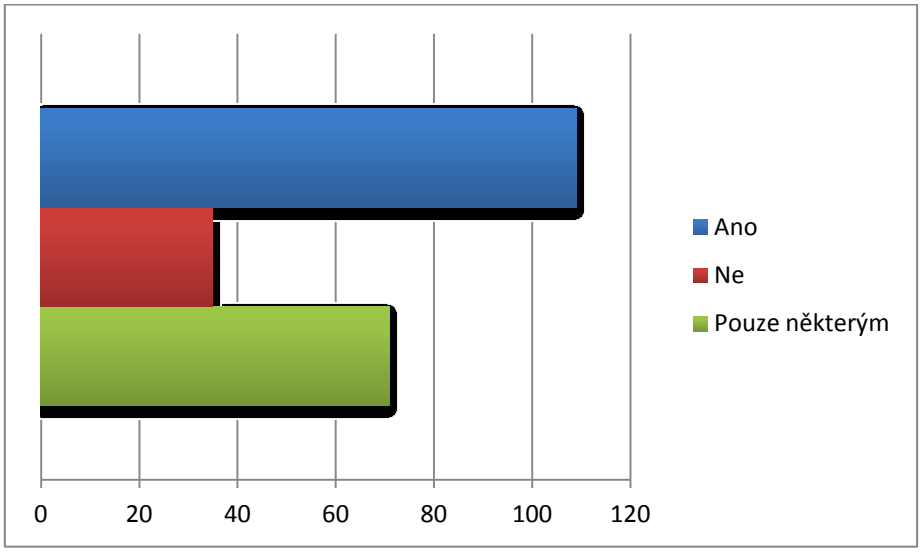
  V podkapitole 3.2.3 byla popsaná oprávnění požadovaná aplikacemi, která se zobrazují uživateli před samotnou instalací. V deváté otázce byli respondenti tázáni, zda si tato oprávnění čtou.



Graf 3.4.4 – Souhrn odpovědí deváté otázky [zdroj: vlastní]

Na grafu výše lze vyčíst převahu kladné odpovědi. Rovných 60% respondentů si oprávnění čte, 37% nikoliv a 3% dotazovaných nikdy žádnou aplikaci neinstalovali.

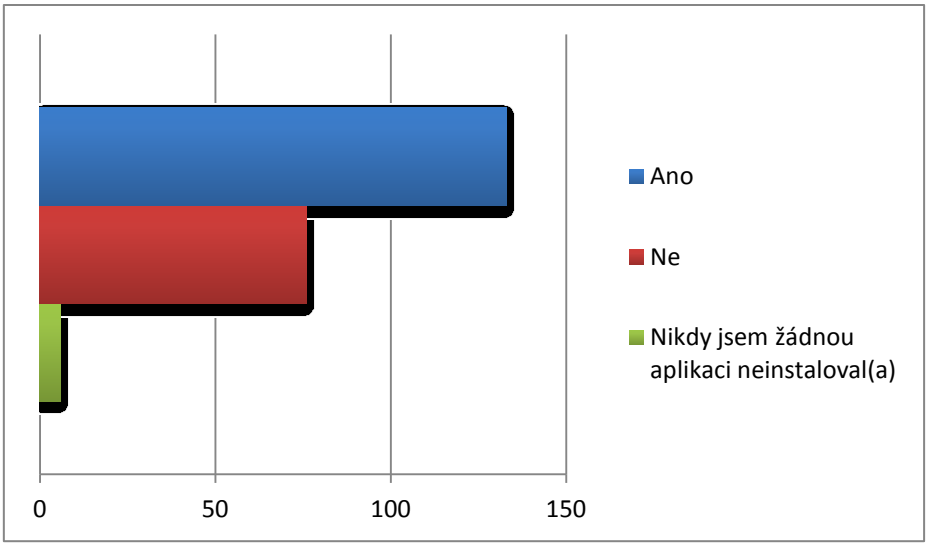
- **Rozumíte těmto oprávněním?**



Graf 3.4.5 - Souhrn odpovědí desáté otázky [zdroj: vlastní]

Pouhých 51% respondentů uvedlo, že požadovaným oprávněním rozumí. Zbývající podíl se dělí mezi ty, kteří jim nerozumí a ty, kteří rozumí pouze některým. Instalace aplikace i přes neznalost oprávnění však může mít vliv na zabezpečení daného zařízení.

- **Odmítl(a) jste již někdy aplikaci instalovat na základě nesouhlasu s potřebným oprávněním?**

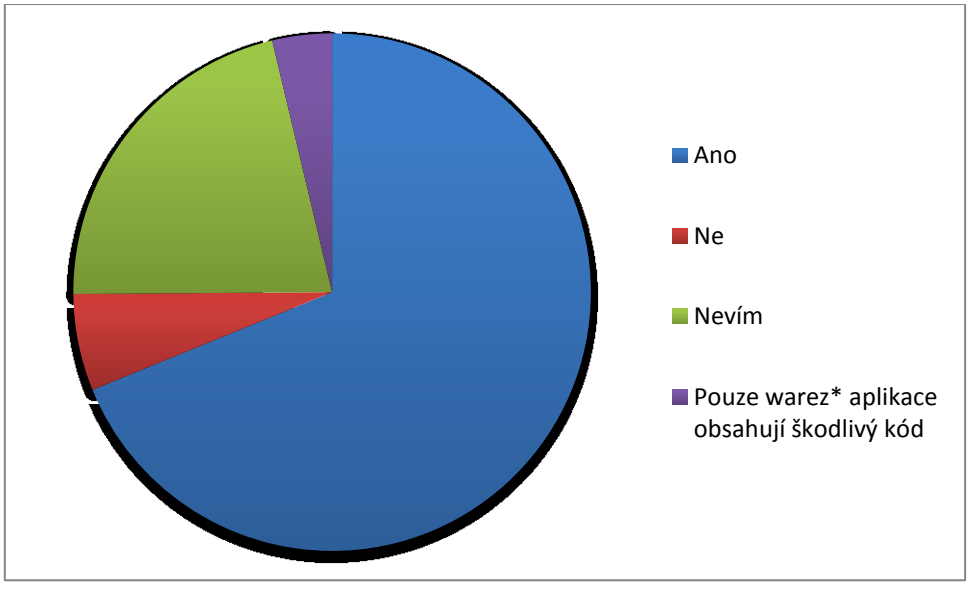


Graf 3.4.6 – Souhrn odpovědí jedenácté otázky [zdroj: vlastní]

I zde, stejně jako u deváté otázky, 3% dotazovaných odpovědělo, že nikdy žádnou aplikaci neinstalovali. Ze zbývajících respondentů 62% odmítlo instalovat aplikaci na základě nesouhlasu s potřebným oprávněním a 35% instalaci vždy povolilo.

- **Myslíte si, že se mohou na oficiální distribuční službě pro OS Android, Google Play, nacházet i aplikace se škodlivým kódem?**

  Poslední, v pořadí dvanáctá, otázka se týkala aplikací obsahujících škodlivý kód umístěných na oficiální distribuční službě pro OS Android, Google Play. V podkapitole 3.3 bylo uvedeno, že k nejčastěji využívanému distribučnímu kanálu škodlivého softwaru patří obchody třetích stran, např. Anzhi.com. Dalším zdrojem jsou diskuzní fóra a webové stránky, na nichž jsou dány k dispozici aplikace k volnému stažení. Většinou se jedná o placené aplikace, které mají odstraněné ochranné prvky, jsou nelegálně šířeny a je tak s nimi nakládáno v rozporu s autorskými právy. Jedním slovem lze tento obsah označit jako warez. Tento pojem byl respondentům vysvětlen v dotazníku v poznámce pod čarou.



Graf 3.4.7 – Souhrn odpovědí dvanácté otázky [zdroj: vlastní]

Většina respondentů, 68%, si myslí, že i na oficiální distribuční službě se mohou vyskytovat aplikace se škodlivým kódem. I přes důslednou kontrolu ze strany Google se v Google Play nacházejí aplikace, které mohou uživatele poškodit, avšak nevyskytují se zde v takové míře, jako ve zmíněných neoficiálních obchodech. Pouhé 4% dotazovaných označilo možnost, že pouze aplikace, které jsou označovány jako warez,

mohou obsahovat škodlivý kód, 21% neví a 6% si myslí, že se na oficiální distribuční službě tyto aplikace nenacházejí.

Závěrem dotazníkového šetření je, že i přes znalost nástrojů ochrany dat a případného rizika, přistupuje většina respondentů k této problematice nezodpovědně a nevyužívá ani základních obranných mechanismů. Z výsledků dotazníkového šetření a studia teoretických zdrojů vyplynul návrh preventivních opatření a doporučení pro práci s OS Android za účelem minimalizace rizik napadení mobilního zařízení.

4 Návrh preventivních opatření a doporučení pro práci s OS Android

Na základě poznatků získaných během studia problematiky bezpečnosti na mobilních zařízeních s operačním systémem Android a vlastního dotazníkového šetření a testování byl sepsán následující návrh doporučení a preventivních opatření pro práci s tímto systémem. Kapitola je rozdělena do dvou částí. První část doporučuje a nabízí uživatelům bližší informace o softwarových nástrojích, které jsou určeny k ochraně dat. Druhá část obsahuje sadu doporučení pro bezpečnou práci se systémem Android.

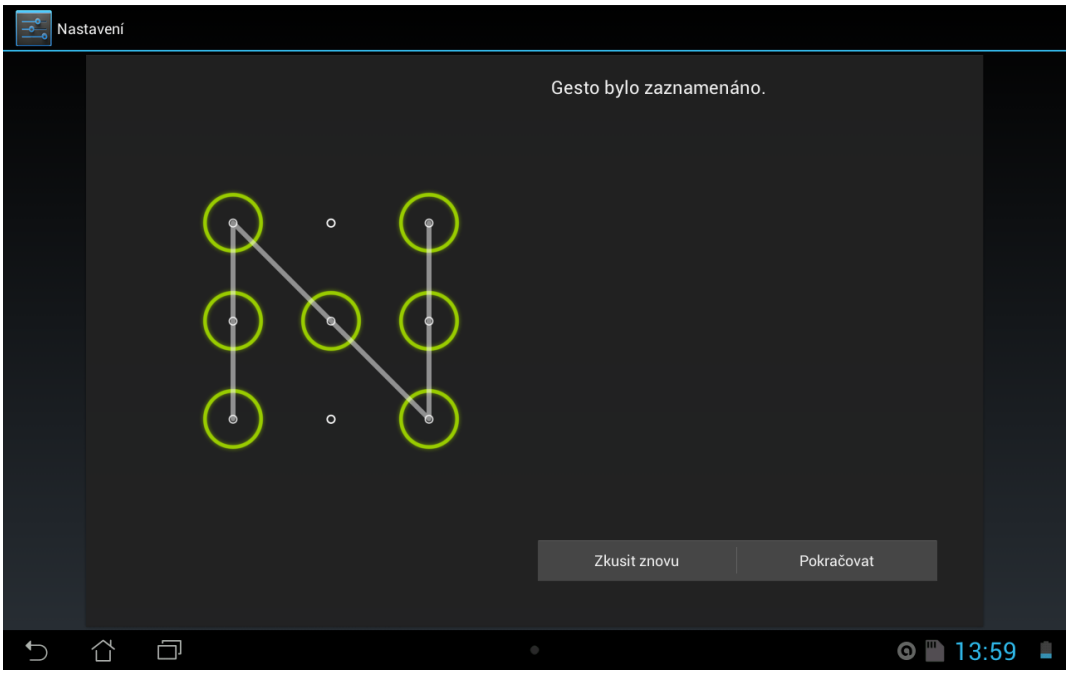
4.1 Doporučené softwarové nástroje určené k ochraně dat

Softwarové nástroje určené pro ochranu dat mohou být:

- součástí systému,
- předinstalovány výrobcem,
- k dodatečnému stažení a instalaci.

Operační systém Android nabízí již ve své základní podobě, tzn. bez nadstaveb výrobce daného zařízení, pokročilé nástroje pro ochranu dat uživatele. Většina je koncipovaná tak, aby znemožnily krádež dat při přímém kontaktu zařízení a útočníka. V nastavení systému lze zvolit požadovanou formu identifikace, která tvoří základ celého bezpečnostního konceptu. Je vhodné, aby byla požadována vždy po startu a každém odemknutí zařízení:

- heslo – kombinace písmen, znaků a čísel,
- PIN – číselné heslo s minimální délkou čtyř čísel,
- gesto – uživatel přejetím prstem po vyznačených bodech vytvoří gesto, viz. Obr. 4.1.1,
- odemknutí obličejem – tato možnost je dostupná v případě, že zařízení disponuje přední kamerou. Data o uživatelově tváři jsou uložena v zařízení a při každém pokusu o odemknutí zařízení je jeho obraz porovnán s uloženými daty. V případě, že uživatel není rozpoznán, je požadováno zadání předem nastaveného číselného hesla. Společnost Google upozorňuje, že se jedná o nejméně bezpečnou metodu v porovnání s výše vyjmenovanými.



Obr. 4.1.1 – Nastavení gesta [zdroj: vlastní]

Výše uvedené možnosti se však stanou nedostupnými, jestliže uživatel využije možnosti zašifrování celého paměťového prostoru zařízení. Odemknout a dešifrovat zařízení bude možné pouze pomocí hesla nebo PINu, bez jejichž zadání nelze zpřístupnit uložená data ani po připojení ke stolnímu počítači prostřednictvím USB kabelu. Změna přístupových hesel je umožněna pouze v případě korektního zadání hesla aktuálního.

V položce zabezpečení v nastavení systému se nachází možnost nastavit Správce zařízení Android. Tato funkce je provázána s Google účtem uživatele, kterému je umožněno při případné ztrátě nebo zcizení zařízení vzdáleně lokalizovat polohu, vzdáleně uzamknout a obnovit tovární, tedy původní, nastavení zařízení za účelem úplného vymazání dat. V případě, že se jedná o smartphone nebo phablet, zobrazí se navíc možnost prozvonění. Podobné nabízí i anti-theft, který je součástí.

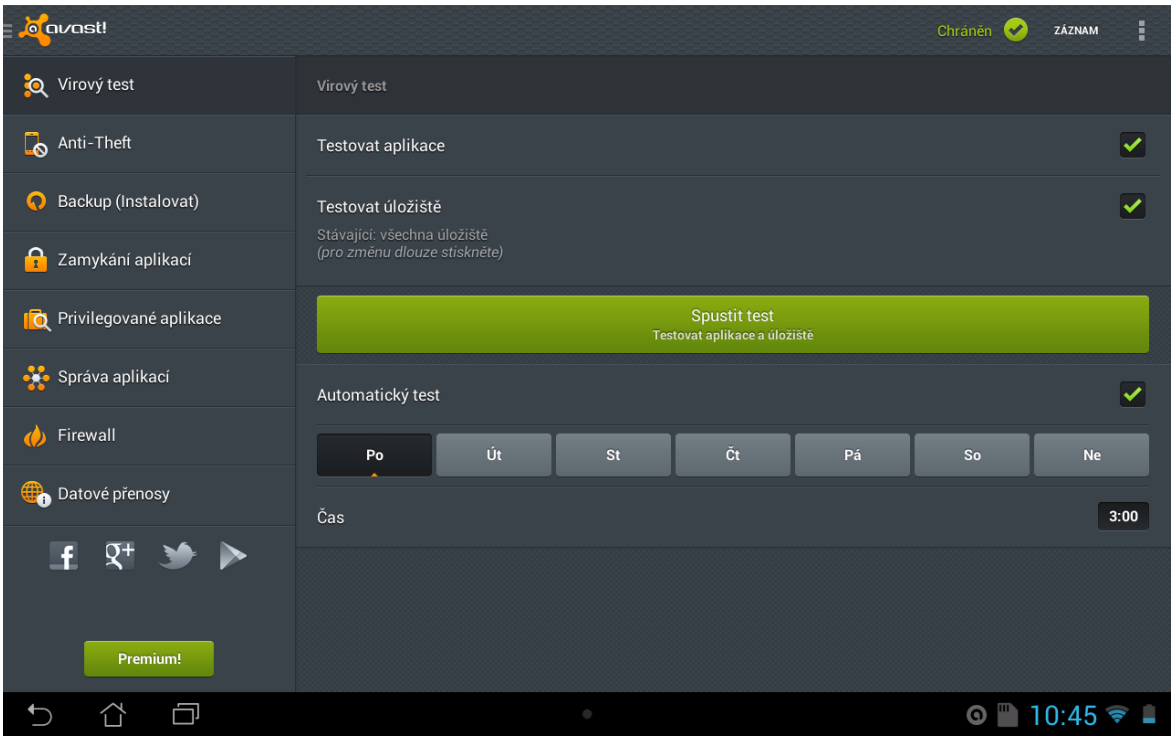
Pokud nejsou na daném zařízení využívány aplikace vyžadující údaje o poloze pro svou správnou funkčnost, pak lze poskytování těchto informací plošně zakázat všem aplikacím a zamezit tak případné špionáži. Tato možnost se rovněž nachází v nastavení systému, v položce Přístup k poloze.

Pokud je povolena instalace aplikací z neznámých zdrojů, zobrazí se při kliknutí možnost přímé instalace prostřednictvím nástroje k instalaci balíčků nebo ověření aplikace a následná instalace. Princip ověřování byl popsán v kapitole 3.2.3. Využití je doporučeno

v případě, že je nevyhnutelně nutné instalovat aplikaci z neověřeného zdroje, např. z důvodu nedostupnosti aplikace v dané zemi v důsledku regionálního omezení.

Mezi nástroje, které mohou být předinstalovány, popř. které si může uživatel dodatečně nainstalovat, patří antivirové a anti-malwarové aplikace, aplikace pro zálohu dat, aplikace informující o požadovaných povoleních již instalovaných aplikací atp. U všech zmíněných nástrojů platí, že by měly být pravidelně aktualizovány.

- Antivirové aplikace - z bezpečnostního hlediska se jedná o minimum, které by mělo obsahovat každé zařízení. Na trhu s mobilními aplikacemi je poměrně široká nabídka, z nichž je velký počet zdarma, a záleží na uživatelových preferencích, kterou antivirovou aplikaci zvolí. Patří zde např. avast! Mobile Security, AVG Anti-Virus, TrustGo Antivirus & Mobile Security. Všechny se vyznačují pokročilými metodami detekce škodlivého softwaru a jsou schopny rozpoznat viry, malware i spyware. Některé navíc obsahují funkci anti-theft, která umožňuje při případné ztrátě nebo krádeži vzdáleně ovládat zařízení pomocí webového rozhraní nebo SMS zpráv. Zařízení tak může být uzamčeno, lokalizováno a mohou z něj být vymazána veškerá data. Placené verze nabízejí fotografování, rozpoznání hlasu zloděje atp. Součástí je i firewall pro blokování přístupu aplikací k internetové síti, avšak pro jeho aktivaci je třeba mít proveden již dříve zmíněný root zařízení.
- Uživatel by měl mít nastaveny automatické aktualizace virové databáze a pravidelné testování paměťového úložiště na přítomnost škodlivého softwaru v době, kdy je zařízení nejméně využíváno, viz. Obr. 4.1.2. Rovněž je vhodné zabezpečit přístup do aplikace pomocí PINu, aby nemohlo být nastavení případným útočníkem změněno.
- Anti-malwarové aplikace – velmi podobně jako antivirové aplikace fungují i aplikace anti-malwarové. Vyjma malwaru detekují a odstraňují spyware, trojské koně a další potenciálně nežádoucí programy. Mezi zástupce lze uvést Malwarebytes Anti-Malware nebo Lookout Security & Antivirus. Pokud se již na daném zařízení nachází antivirus, prakticky nevzniká potřeba instalovat také anti-malwarovou aplikaci. Pokud se však uživatel pro instalaci rozhodne, platí zde rovněž, že je důležité pravidelně aktualizovat databázi škodlivého softwaru.



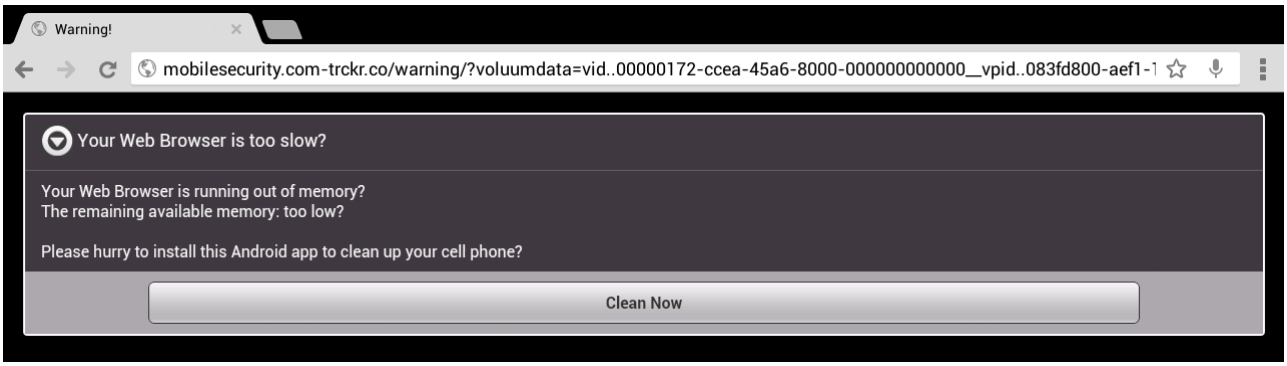
Obr. 4.1.2 – Uživatelské rozhraní antivirové aplikace avast! Mobile security [zdroj: vlastní]

- Aplikace pro zálohu dat – ztráta kontaktů může mít velký dopad, zvláště v případě ztráty kontaktů na obchodní partnery. Je proto vhodné provádět pravidelné zálohy alespoň jednou měsíčně pomocí k tomu určené aplikace, kterou může být např. Ultimate Backup, Titanium Backup, avast! Mobile Backup atp. Aplikace umožňují zálohovat kromě zmíněných kontaktů také SMS a MMS zprávy, záložky webového prohlížeče, události kalendáře, systémové nastavení, záznamy o telefonních hovorech, ale také aplikace a multimediální obsah. Záloha může být uložena na paměťovou kartu zařízení nebo pomocí technologie cloudového řešení nahrána na server, odkud je dostupná pro případnou obnovu dat. Celý proces zálohování probíhá v uživatelsky přívětivém prostředí a neměl by představovat problém ani pro méně zkušené uživatele.
- Aplikace informující o požadovaných povoleních instalovaných aplikací - problematika oprávnění aplikací byla rozepsána v kapitole 3.2.3. Pokud chce uživatel ověřit, která oprávnění jsou aplikacemi využívány, může tak učinit, např. pomocí aplikace F-Secure App Permissions, a odhalit tak nežádoucí software.

4.2 Doporučení pro práci s OS Android

Kromě využívání softwarových nástrojů je pro dosažení vyššího stupně zabezpečení zapotřebí, aby uživatel dodržel při práci s OS Android následující sadu doporučení:

- systém udržovat v aktuální verzi vydané výrobcem zařízení,
- při připojování do nezabezpečené veřejné Wi-Fi sítě nepoužívat služby obsahující citlivá hesla, např. internet banking,
- vyvarovat se stránkám s podezřelým obsahem,
- instalovat aplikace pouze z oficiálních zdrojů a před instalací si přečíst recenze a hodnocení dané aplikace ostatními uživateli,
- během instalace nových aplikací se snažit porozumět veškerým požadovaným oprávněním a uvážit, zda jsou opravdu všechna potřebná pro správnou funkčnost aplikace, pokud např. požaduje aplikace pro úpravu fotografií oprávnění na čtení kontaktů a zasílání SMS zpráv bez vědomí uživatele, které jsou zřejmě nad rámec zajištění správné funkčnosti, bylo by vhodné vyhledat alternativní aplikaci,
- neklikat na odkazy obsažené v SMS nebo e-mailových zprávách pocházejících z podezřelého zdroje a na odkazy uvedené na webových stránkách vybízející např. k instalaci aplikace určené k uvolnění operační paměti zařízení, viz. Obr. 4.2.1,



Obr. 4.2.1 – Příklad odkazu s podezřelým obsahem [zdroj: vlastní]

- v nastavení zařízení deaktivovat „vývojářský mód“, pokud je dostupný, a také možnost instalace aplikací třetích stran,
- vypínat Wi-Fi, Wi-Fi direct a Bluetooth připojení pokud není aktivně využíváno

- mít využívaný webový prohlížeč aktualizovaný na nejnovější verzi a nemít v paměti uložena hesla pro webové služby,
- neuchovávat citlivá data na externí paměťové kartě,
- pokud je v daném zařízení proveden root, který není doporučen méně zkušeným uživatelům, práva administrátora by neměla být přidělena libovolné aplikaci,
- pokud je pozorováno neobvyklé chování zařízení, např. rychlé vybíjení baterie, je vhodné, analyzovat zdroj problému pomocí položky Baterie v nastavení systému a ručně zadat okamžitou kontrolu příslušnou antivirovou aplikací,
- v případě, že nejsou využívány služby tzv. premium SMS, lze je zcela zakázat, popř. nastavit u mobilního operátora jejich denní limit a zamezit tak nechtěným finančním ztrátám.

Při dodržení výše uvedených doporučení a nainstalovaném softwaru na ochranu dat je riziko napadení mobilního zařízení škodlivým softwarem minimalizováno.

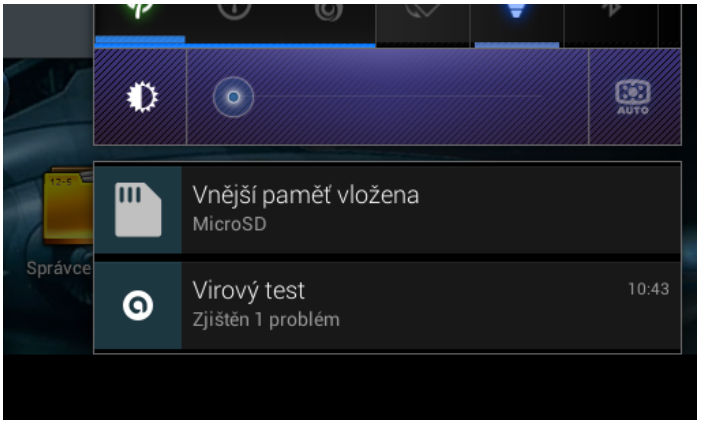
5 Vyhodnocení efektu z realizace opatření

Pro ověření efektu realizace navrhovaných opatření bylo provedeno testování, které probíhalo po dobu šesti týdnů. K dispozici byly dvě mobilní zařízení - smartphone Meizu M9 s verzí systému 4.0.4 Ice Cream Sandwich a tablet Asus MeMO Pad Smart ME301T s verzí systému 4.2.1 Jelly Bean.

Veškerá data smartphonu byla předem zálohována na externí paměťové médium pomocí aplikace My Backup Pro. Následně byl odinstalován antivirový a anti-malwarový software. Kontakty, fotografie, e-mailové a SMS zprávy, položky kalendáře a účty sociálních sítí byly vymazány za účelem ochrany vlastních dat a byly nahrazeny daty smyšlenými. Během doby testování bylo běžně využíváno internetové připojení prostřednictvím Wi-Fi a 3G sítí a navštěvovány webové stránky. Rovněž byly využívány služby aplikací jako např. internetové rádio a jiné, které vyžadují ke svému chodu připojení k datové síti a instalovány hry z neoficiálních zdrojů. Během třetího až pátého týdne testování došlo k pozorovatelnému zpomalení systému, které se projevovalo opožděnými reakcemi na požadavky uživatele. Z tohoto důvodu muselo být zařízení občasně restartováno za účelem ukončení určitých procesů a uvolnění operační paměti. V šestém týdnu testování došlo k zamrznutí systému při spuštěné aplikaci internetového rádia a aktivovaných datových přenosech. Přístroj nereagoval na hardwarové tlačítko pro zapnutí, které při dlouhém stisku slouží rovněž jako tlačítko pro resetování. Po vyjmutí a opětovném vložení baterie a zapnutí přístroje se zobrazilo pouze logo výrobce, ale systém samotný nenastartoval. Jedinou možností na obnovu funkčnosti bylo umístění aktualizačního balíčku na paměťovou kartu a jeho spuštění pomocí stisknutí dvou hardwarových tlačítek najednou, neboli dvojhmatu. Systém byl přeinstalován a veškerá data smazána. Poté byla nainstalována antivirová a anti-malwarová aplikace a obnovena záloha dat. Po ukončení testování byl smartphone nadále používán bez příznaků napadení škodlivým softwarem.

Na druhém zařízení, tabletu, byla instalována antivirová aplikace avast! Mobile security ve které byly nastaveny automatické aktualizace virové databáze a pravidelné testování paměťového úložiště, zakázána instalace aplikací z neznámých zdrojů a aktualizován webový prohlížeč Google Chrome. Při návštěvě určitých webových stránek opakovaně docházelo k samovolnému stahování aplikací do paměti tabletu. Instalovaný antivirový program

automaticky analyzoval stažený soubor jako škodlivý software a pomocí notifikace na to upozornil, viz. Obr. 5.1.1, a navrhnul řešení v podobě jeho vymazání z paměti. Během doby testování nebyly jiné problémy zaznamenány.



Obr. 5.1.1 – Detekce škodlivého softwaru [zdroj: vlastní]

Z poznatků získaných testováním vyplynulo, že bez využití aplikací pro ochranu dat a datových sítí se zvyšuje riziko napadení zařízení škodlivým softwarem. Pokud uživatel nenavštěvuje prostřednictvím mobilního zařízení webové stránky ani jinak nevyužívá datových sítí, pravděpodobnost nakažení škodlivými aplikacemi a případná ztráta dat se minimalizuje. Zde je ale třeba mít na vědomí fakt, že mobilní zařízení, zejména tablety, byla záměrně vyvinuta pro komunikaci pomocí internetové sítě a prohlížení webového obsahu a nelze tedy očekávat, že bude tato funkcionalita uživateli opomíjena.

6 Závěr

Během velmi krátké doby došlo k rozšíření systému Android natolik, že se stal nejpoužívanějším mobilním operačním systémem na světě. Právě jeho rozšíření a implementace i do levných zařízení je důsledkem politiky uplatňované vývojáři, kteří poskytují zdrojový kód jako open-source. Masová popularita mezi uživateli má za následek, že někteří jsou vlastníky dvou i více zařízení pracujících na platformě Android, která se stala běžnou součástí jejich každodenních životů. Mezi uloženými daty se nachází telefonní čísla, e-maily a také fotografie, jejichž ztráta je nežádoucí událostí, která může zkomplikovat i profesní život uživatele. Také v každé firmě či společnosti se nachází mobilní zařízení s daty, jejichž zcizení nebo vymazání by mohlo znamenat cenné ztráty. Nemusí se však jednat pouze o zařízení používaná členy vrcholového managementu a proto je vhodné, aby byla této problematice věnovaná patřičná pozornost. Cílem diplomové práce bylo analyzovat bezpečnost mobilního operačního systému Android a upozornit na škodlivý software, který může ohrozit data uložená v mobilních zařízeních. Součástí práce je vlastní dotazníkové šetření, testování a návrh preventivních opatření a doporučení.

Pro zajištění nejširšího možného vzorku respondentů byl dotazník distribuován v tištěné a elektronické podobě. Dotazníkové šetření přineslo překvapivé výsledky. Povědomí uživatelů o nástrojích ochrany dat a riziku jejich ztráty je v kontrastu s počtem uživatelů, kteří tyto nástroje používají. Jako vysvětlení se nabízí mylná domněnka uživatelů, že se tzv. „ztratí v davu“ a nabývají tak dojmu, že jejich identita a data nejsou pro případné útočníky zajímavá. Druhou možností je, že se uživatel domnívá, že i přes napadení zařízení nemá co ztratit. V takovém případě si není vědom hodnoty svých dat.

Na základě poznatků získaných studiem dané problematiky a dotazníkového šetření byly sepsány návrhy a doporučení pro minimalizaci rizika nakažení mobilních zařízení škodlivými aplikacemi. Kromě softwarových nástrojů byla uvedena i preventivní doporučení pro práci s OS Android za účelem ochrany dat. Uvedená opatření jsou z časového hlediska nenáročná na zavedení. Vzhledem k rozsáhlé nabídce softwarových nástrojů poskytovaných zdarma jsou nenáročná také na finanční zdroje. Je důležité podotknout, že se nejedná o složité operace a neměly by tak činit potíže ani méně zkušeným uživatelům.

Závěrečné testování efektu realizace opatření na dvou mobilních zařízeních, které probíhalo po dobu šesti týdnů, prokázalo přítomnost rizika napadení zařízení a případného zcizení dat. U prvního, nechráněného mobilního zařízení, docházelo ke zpomalování rychlosti odezvy systému a jeho restartování až do úplného selhání a ztráty dat. Druhé zařízení, chráněné antivirovou aplikací, bylo provozováno v souladu s doporučeními pro práci uvedenými ve čtvrté kapitole, a nebyly pozorovány výkyvy výkonu ani cokoliv jiného, co by nasvědčovalo napadení zařízení. Po provedeném průzkumu a analýze získaných dat z dotazníkového šetření, vypracování návrhu řešení bezpečnostních opatření a testování efektu z realizace těchto opatření, lze konstatovat, že veškeré cíle stanovené v úvodu diplomové práce byly splněny.

Podle prognóz předních společností v oboru bezpečnosti v IT nelze v roce 2014 očekávat pokles zájmu vývojářů škodlivého softwaru o platformu Android. To může být důsledkem rostoucí produkce mobilních zařízení s tímto operačním systémem, na které se významně podílí činští výrobci používající ve svých produktech starší verze systému, jejíž bezpečnostní chyby jsou veřejně známy. Přímou úměrou tak získává na významu studium a průzkum dané problematiky a šíření výsledků o potenciálním riziku mezi širokou veřejnost.

Seznam použité literatury

Monografické zdroje:

1. HOOG, Andrew. *Android forensics: Investigation, Analysis, and Mobile Security for Google Android*. Waltham, MA: Syngress, 2011, 372 s. ISBN 978-1-59749-651-3.
2. DUBEY, Abhishek a Anmol MISRA. *Android Security: Attacks and Defenses*. Boca Raton, FL: CRC Press, 2013, 280 s. ISBN 978-143-9896-464.
3. GUNASEKERA, Sheran A. *Android Apps Security*. New York, NY: Apress, 2012, 248 s. ISBN 978-143-0240-631.
4. SIX, Jeff. *Application Security for the Android Platform*. Sebastopol, CA: O'Reilly Media, Inc., 2012, 114 s. ISBN 14-493-1507-0.
5. VÁVRŮ, Jiří a Miroslav UJBÁNYAI. *Programujeme pro Android*. 2., rozš. vyd. Praha: Grada, 2013, 256 s. ISBN 978-80-247-4863-4.

Elektronické zdroje:

6. APPLE INC. *IOS Security* [pdf]. Apple Inc. [cit. 6.3.2014]. Dostupné z: http://images.apple.com/iphone/business/docs/iOS_Security_Feb14.pdf
7. GRUSH, Andrew. *Nymi bracelet uses your heartbeat to unlock your devices* [online]. Android Authority [cit. 22.1.2014]. Dostupné z: http://www.androidauthority.com/nymi-261898/
8. Android Developers. *Manifest permission group* [online]. Android Developers [cit. 11.3.2014]. Dostupné z: http://developer.android.com/reference/android/Manifest.permission_group.html
9. KRČMÁŘ, Petr. *Aktualizační systém Androidu umožňuje aplikacím potichu navýšit práva* [online]. Root.cz [cit. 29.3.2014]. Dostupné z: http://www.root.cz/zpravicky/aktualizacni-system-androidu-umoznuje-aplikacim-potichu-navysit-prava/
10. Kaspersky Lab. Počet *škodlivých aplikací pro Android dosáhl deseti milionů* [online]. Kaspersky Lab [cit. 30.3.2014]. Dostupné z: http://www.kaspersky.com/cz/about/news/virus/2014/pocet-skodlivych-aplikaci-pro-Android-dosahl-deseti-milionu
11. F-SECURE. *Threat Report H2 2013* [pdf]. F-Secure [cit. 14.3.2014]. Dostupné z: http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H2_2013.pdf
12. FORTINET. *2014 Threat Landscape Report* [pdf]. Fortinet [cit. 15.3.2014]. Dostupné z: http://www.fortinet.com/sites/default/files/whitepapers/Threat-Landscape-2014.pdf

13. ESET. *Trends for 2014: The Challenge of Internet Privacy* [pdf]. ESET [cit. 15.3.2014]. Dostupné z: http://www.welivesecurity.com/wp-content/uploads/2013/12/Annual-Threat-Trends-Predictions-2014.pdf
14. Computerworld. *Apple aktualizoval whitepaper systému* iOS [online]. Computerworld [cit. 16.2.2014]. Dostupné z: http://computerworld.cz/securityworld/apple-aktualizoval-whitepaper-systemu-ios-50896

Odborná periodika:

15. *CHIP: magazín informačních technologií*. Praha: Vogel Publishing, 2012, roč. 22, č. 2. ISSN 1210-0684.
16. *CHIP: magazín informačních technologií*. Praha: Vogel Publishing, 2013, roč. 23, č. 2, 8, 10, 11. ISSN 1210-0684.
17. *CHIP: magazín informačních technologií*. Praha: Vogel Publishing, 2013, roč. 24, č. 1. ISSN 1210-0684.

Seznam zkratek a pojmů

3D	trojrozměrné (zobrazení objektu)
3G síť	síť umožňující přenášet telefonní hovory i data
Bluetooth	technologie určená pro bezdrátovou komunikaci propojující dvě a více elektronických zařízení
Cloud	pronajímaný hardware nebo software (formou služby)
Desktopové OS	operační systémy určené pro stolní počítače a notebooky
Display	obrazovka zařízení
E-mail	elektronická pošta zasílaná pomocí internetového připojení
GPS	Global Positioning System, globální družicový polohový systém pro určení přesné polohy
Konsorcium	společenství
MMS	Multimedia Messaging System, multimediální zpráva, přenáší text, fotografie, audio a video soubory
Open-source	software s otevřeným zdrojovým kódem, technicky i legálně dostupný, uživatelům je umožněno ho upravovat
OS	Operating System, operační systém
PIN	Personal Identification Number, identifikační číslo pro identifikaci jeho držitele
Premium SMS	SMS zprávy, jejichž cena je odlišná od běžných SMS zpráv
Root	systémový superuživatel, disponuje nejvyššími možnými oprávněními
SMS	Short Message Service, krátká textová zpráva
Warez	autorská díla, se kterými je nakládáno nelegálně, zejména v rozporu s autorským právem

Wi-Fi	označení standardů popisujících bezdrátovou komunikaci v počítačové síti
Wi-Fi direct	technologie umožňuje propojit dvě zařízení bez nutnosti použití Wi-Fi routeru

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byl seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 25. 4. 2014

.....

Bc. Ondřej Gajda

Seznam příloh

Příloha č1. Dotazník

Dobrý den,

tento krátký formulář, na jehož vyplnění stačí méně než 5 minut, slouží jako podklad pro mou diplomovou práci na téma: "Bezpečnost na mobilních zařízeních s operačním systémem Android".

Prosím o vyplnění pouze v případě, že vlastníte mobilní zařízení (mobilní telefon, tablet, notebook atp.) právě s operačním systémem Android. Rovněž prosím o svědomité vyplnění všech údajů. Dotazník je 100% anonymní.

Děkuji všem, kteří se rozhodnou dotazník vyplnit.

*Povinné pole

1. Pohlaví? *

První dvě otázky slouží pouze pro získání přehledu o vzorku respondentů.

- ○ Muž
- ○ Žena

2. Váš věk? *

První dvě otázky slouží pouze pro získání přehledu o vzorku respondentů.

- ○ 0-15 let
- ○ 16-20 let
- ○ 21-32 let
- ○ 33-40 let
- ○ 41-50 let
- ○ 50 a více let

3. Zajímal(a) jste se někdy o problematiku bezpečnosti na mobilních zařízeních? *

- ○ Ano
- ○ Ne

4. Existují podle vašeho názoru nějaké hrozby pro běžné uživatele, kteří nijak nezasahují do samotného operačního systému (např. nemají proveden root* na svém zařízení)? *

* ROOT umožňuje spustit danou aplikaci jako superuživatel, na normální aplikace to vliv nemá. Existují však aplikace, které toho umí využít a dají uživateli nové možnosti (např. mazat / upravovat soubory na systémovém oddílu)

- ○ Ano
- ○ Ne
- ○ Nevím

5. Jaké obranné mechanismy znáte (můžete označit více možností) *

- ☐ Antivirus
- ☐ Anti-Theft
- ☐ Antimalware
- ☐ žádné
- ☐ Jiné:

6. Jaké obranné mechanismy používáte (můžete označit více možností) *

- ☐ Antivirus
- ☐ Anti-Theft
- ☐ Antimalware
- ☐ žádné
- ☐ Jiné:

7. Zálohujete v pravidelných intervalech svá data (kontakty, SMS zprávy, kalendář aj.)? *

- ○ Ano
- ○ Ne

8. Přišel/přišla jste již někdy o svá data (kontakty, SMS zprávy, kalendář aj.)? *

- ○ Ano
- ○ Ne

9. Čtete si potřebná oprávnění pro běh aplikace při její instalaci? *

Tato oprávnění se zobrazují ještě před samotným stažením aplikace do telefonu prostřednictvím Google Play. Pokud je aplikace instalována přímo z telefonu (např. paměťové karty) zobrazí se seznam potřebných oprávnění při instalaci.

- Ano
- Ne
- Nikdy jsem žádnou aplikaci neinstaloval(a)

10. Rozumíte těmto oprávněním? *

Viz. otázka č.9

- Ano
- Ne
- Pouze některým

11. Odmítl(a) jste již někdy aplikaci instalovat na základě nesouhlasu s potřebným oprávněním? *

- Ano
- Ne
- Nikdy jsem žádnou aplikaci neinstaloval(a)

12. Myslíte si, že se mohou na oficiální distribuční službě pro OS Android, Google Play, nacházet i aplikace se škodlivým kódem? *

*Warez je termín počítačového slangu označující autorská díla, se kterými je nakládáno nelegálně, zejména v rozporu s autorským právem (jinými slovy načerno stažená aplikace z internetu)

- Ano
- Ne
- Nevím
- Pouze warez* aplikace obsahují škodlivý kód